深信服智安全
SANGFOR SECURITY

风险评估报告

深信服科技股份有限公司

报告生成时间：2025-02-19 22:01:52

1 综述

本次评估的总体安全等级为高危

资产情况如下：

- 共检测到存活资产5个，其中，存在风险的资产5个。

攻击面情况如下：

- 漏洞共44个，其中严重0个，高危11个，中危14个，低危19个。
- 弱口令共0个。
- 登录入口共0个，其中web登录入口0个，系统登录入口0个。

若存在严重或高危风险,建议您重点关注并及时修复。

2 资产统计

2.1 资产基本信息

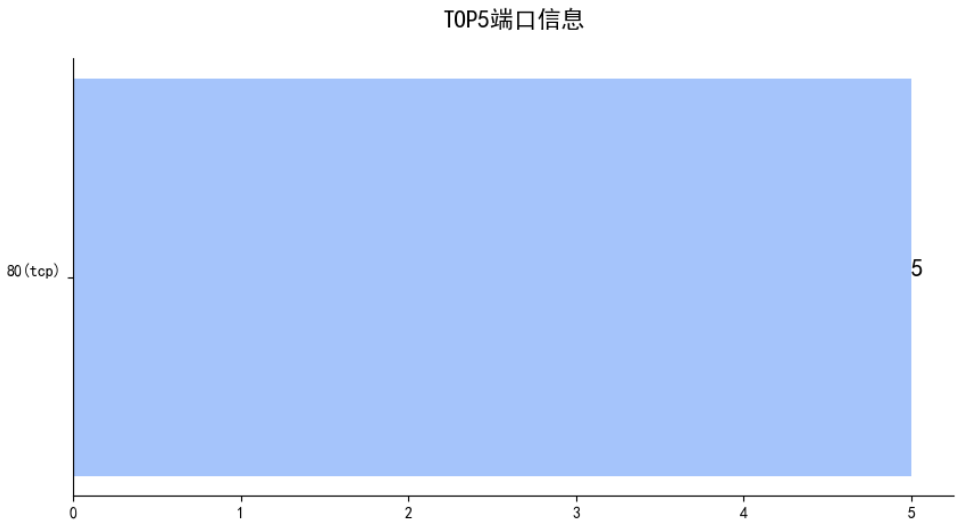
本次共检测到存活资产5个，其中，主机资产0个，网站资产5个。

资产基本信息情况如下表所示：

序号	IP/URL	设备类型	操作系统	资产名称	是否核心	责任人	业务组
1	http://byw3133480001.my3w.com	服务器设备			否		
2	http://th-info.com	未知			否		
3	http://th-storage.com	服务器设备			否		
4	http://www.th-info.com	服务器设备			否		
5	http://www.th-storage.com	服务器设备			否		

2.2 资产端口信息

存在端口开放的资产共5个，开放最多的端口为80(tcp)，开放端口数量最多的资产为http://byw3133480001.my3w.com。TOP5端口使用情况如下图所示：



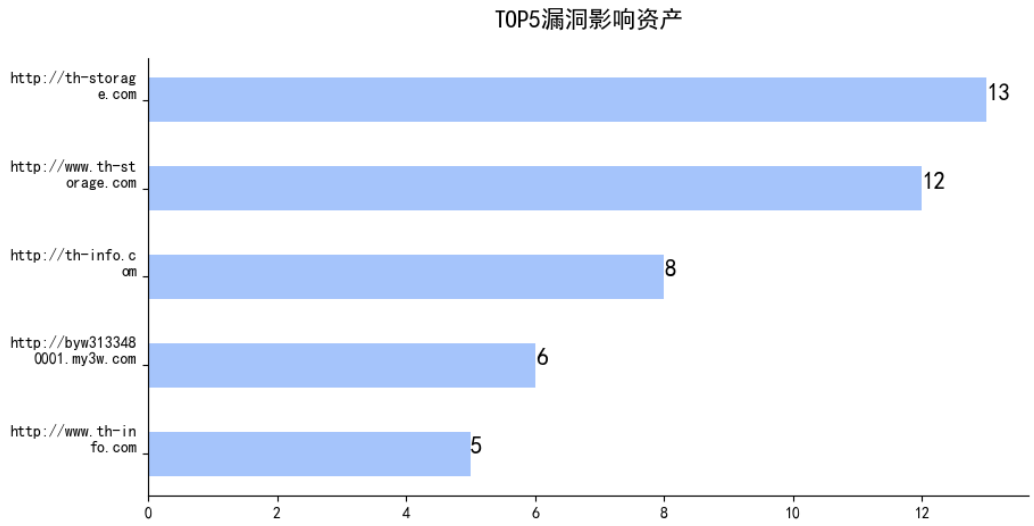
资产端口信息如下表所示：

序号	IP/URL	端口数	端口	协议	服务	软件
1	http://byw3133480001.my3w.com	1	80	tcp	http	http
2	http://th-info.com	1	80	tcp	http	http
3	http://th-storage.com	1	80	tcp	http	http
4	http://www.th-info.com	1	80	tcp	http	http
5	http://www.th-storage.com	1	80	tcp	http	http

2.3 资产风险信息

2.3.1 漏洞

存在风险的资产共5个，其中风险数量最多的资产TOP5如下图所示：



资产的漏洞风险情况如下表所示：

序号	IP/URL	严重	高	中	低	总计
1	http://th-storage.com	0	2	6	5	13
2	http://www.th-storage.com	0	3	3	6	12
3	http://th-info.com	0	4	3	1	8
4	http://byw3133480001.my3w.com	0	2	2	2	6
5	http://www.th-info.com	0	0	0	5	5

2.3.2 弱口令

本次评估未发现存在弱口令风险的资产。

2.3.3 登录入口

本次评估未发现存在登录入口风险的资产。

3 资产详情

3.1 http://th-storage.com

3.1.1 资产基本信息

资产	http://th-storage.com
是否核心	否
资产名称	
业务组	
责任人	
所属部门	
联系电话	
解析ip	182.92.96.197
网站标题	文档已移动
应用	None
中间件	http
数据库	-
开发语言	-
开发框架	-

3.1.2 资产端口信息

序号	开放端口	协议	开放服务	软件信息	网站URL	网站标题
1	80	tcp	http	http	http://th-storage.com	文档已移动

3.1.3 资产风险信息

该资产总体安全等级为高危，不同类型的风险分布如下：

风险类型	严重	高	中	低	总计
系统漏洞	0	2	1	0	3
web漏洞	0	0	5	5	10
弱口令	0	0	0	0	0
web登录入口	0	0	0	0	0
系统登录入口	0	0	0	0	0
总计	0	2	6	5	13

3.2 http://www.th-storage.com

3.2.1 资产基本信息

资产	http://www.th-storage.com
是否核心	否
资产名称	
业务组	
责任人	
所属部门	
联系电话	
解析ip	182.92.96.197
网站标题	北京同方光盘股份有限公司
应用	None
中间件	http
数据库	-
开发语言	-
开发框架	-

3.2.2 资产端口信息

序号	开放端口	协议	开放服务	软件信息	网站URL	网站标题
1	80	tcp	http	http	http://www.th-storage.com	北京同方光盘股份有限公司

3.2.3 资产风险信息

该资产总体安全等级为高危，不同类型的风险分布如下：

风险类型	严重	高	中	低	总计
系统漏洞	0	2	1	0	3
web漏洞	0	1	2	6	9
弱口令	0	0	0	0	0
web登录入口	0	0	0	0	0
系统登录入口	0	0	0	0	0
总计	0	3	3	6	12

3.3 http://th-info.com

3.3.1 资产基本信息

资产	http://th-info.com
是否核心	否
资产名称	
业务组	
责任人	
所属部门	
联系电话	
解析ip	182.92.96.197
网站标题	
应用	None
中间件	http
数据库	-
开发语言	-
开发框架	-

3.3.2 资产端口信息

序号	开放端口	协议	开放服务	软件信息	网站URL	网站标题
1	80	tcp	http	http	http://th-info.com	

3.3.3 资产风险信息

该资产总体安全等级为高危，不同类型的风险分布如下：

风险类型	严重	高	中	低	总计
系统漏洞	0	2	1	0	3
web漏洞	0	2	2	1	5
弱口令	0	0	0	0	0
web登录入口	0	0	0	0	0
系统登录入口	0	0	0	0	0

总计	0	4	3	1	8

3.4 http://byw3133480001.my3w.com

3.4.1 资产基本信息

资产	http://byw3133480001.my3w.com
是否核心	否
资产名称	
业务组	
责任人	
所属部门	
联系电话	
解析ip	182.92.96.197
网站标题	
应用	None
中间件	http
数据库	-
开发语言	-
开发框架	-

3.4.2 资产端口信息

序号	开放端口	协议	开放服务	软件信息	网站URL	网站标题
1	80	tcp	http	http	http://byw3133480001.my3w.com	

3.4.3 资产风险信息

该资产总体安全等级为高危，不同类型的风险分布如下：

风险类型	严重	高	中	低	总计
系统漏洞	0	2	1	0	3
web漏洞	0	0	1	2	3

弱口令	0	0	0	0	0
web登录入口	0	0	0	0	0
系统登录入口	0	0	0	0	0
总计	0	2	2	2	6

3.5 http://www.th-info.com

3.5.1 资产基本信息

资产	http://www.th-info.com
是否核心	否
资产名称	
业务组	
责任人	
所属部门	
联系电话	
解析ip	182.92.96.197
网站标题	文档已移动
应用	None
中间件	http
数据库	-
开发语言	-
开发框架	-

3.5.2 资产端口信息

序号	开放端口	协议	开放服务	软件信息	网站URL	网站标题
1	80	tcp	http	http	http://www.th-info.com	文档已移动

3.5.3 资产风险信息

该资产总体安全等级为低危，不同类型的风险分布如下：

风险类型	严重	高	中	低	总计
系统漏洞	0	0	0	0	0
web漏洞	0	0	0	5	5
弱口令	0	0	0	0	0
web登录入口	0	0	0	0	0
系统登录入口	0	0	0	0	0
总计	0	0	0	5	5

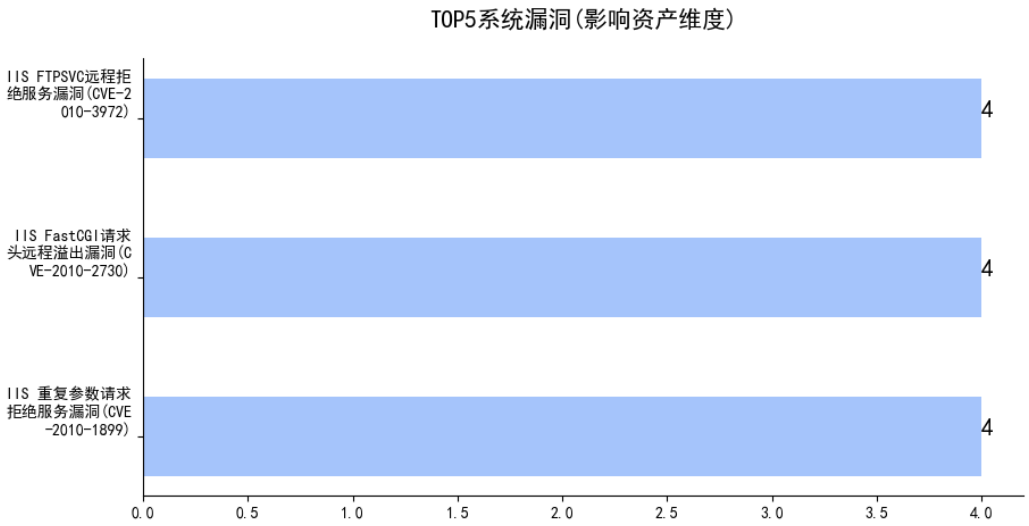
4 风险统计

4.1 系统漏洞影响分析

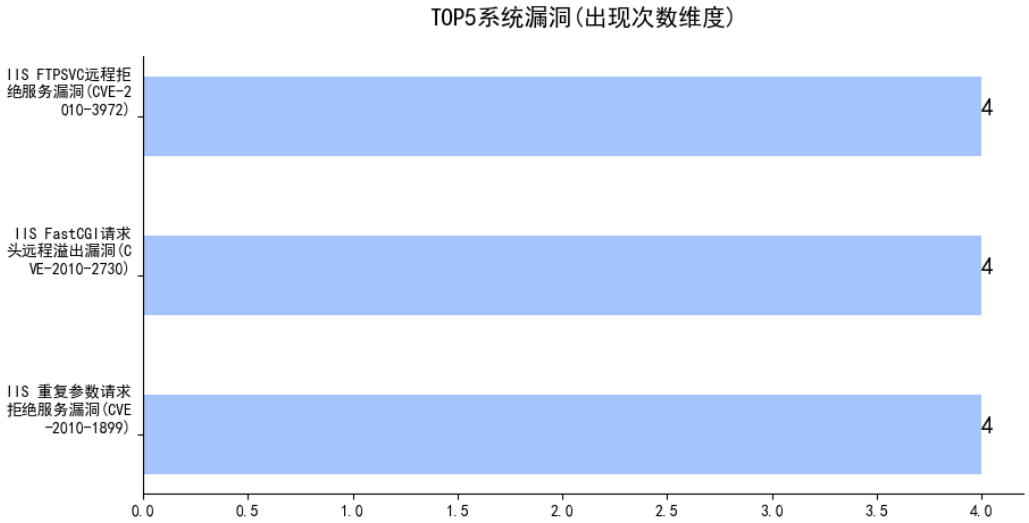
4.1.1 风险等级分析

4.1.2 影响资产分析

系统漏洞影响资产数量TOP5统计如下：



出现次数指的是每个漏洞影响的端口或页面数量，系统漏洞出现次数TOP５统计如下：



TOP100系统漏洞影响资产情况如下表所示：

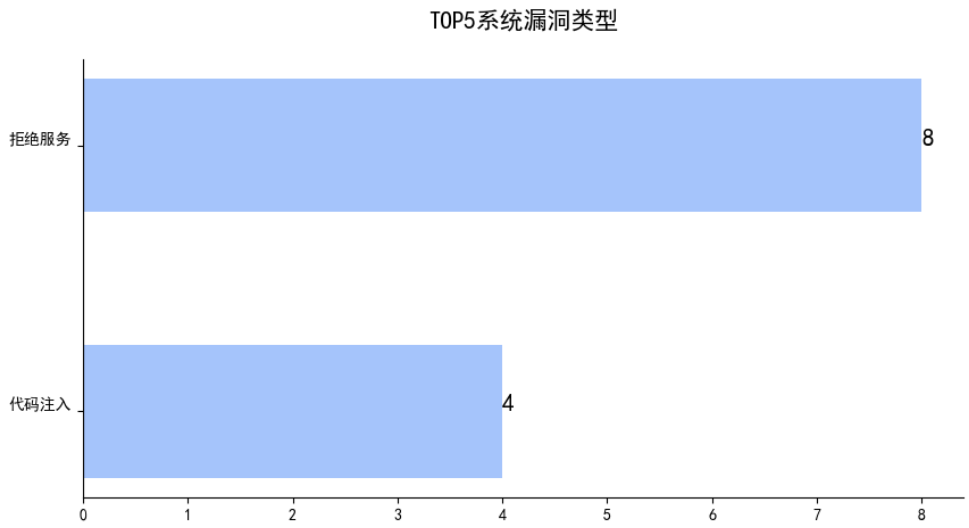
注：此处仅展示TOP100系统漏洞及其影响资产情况，每个风险影响的资产最多展示10个，更多信息请登录平台查看，或者下载excel/html报告查看。

序号	系统漏洞名称	风险等级	影响资产(仅展示10个)	影响资产数	出现次数
1	IIS FTPSVC远程拒绝服务漏洞(CVE-2010-3972)	高	http://th-info.com http://www.th-storage.com http://byw3133480001.my3w.com http://th-storage.com	4	4
2	IIS FastCGI请求头远程溢出漏洞(CVE-2010-2730)	高	http://th-info.com http://www.th-storage.com http://byw3133480001.my3w.com http://th-storage.com	4	4

3	IIS 重复参数请求拒绝服务漏洞(CVE-2010-1899)	中	http://th-info.com http://www.th-storage.com http://byw3133480001.my3w.com http://th-storage.com	4	4

4.1.3 风险类型分析

系统漏洞类别TOP５统计如下：



系统漏洞类别TOP５统计如下：

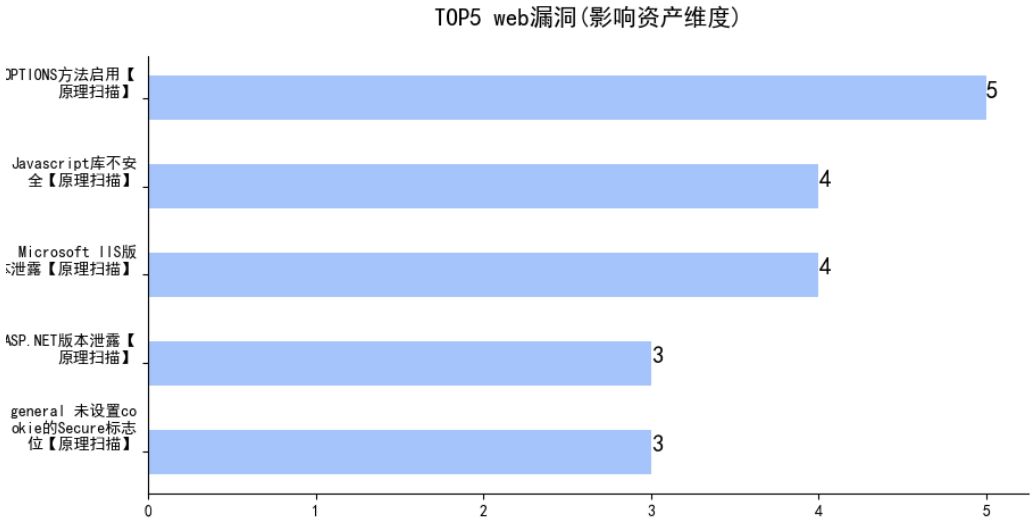
序号	漏洞名称	出现次数
1	拒绝服务	8
2	代码注入	4

4.2 web漏洞影响分析

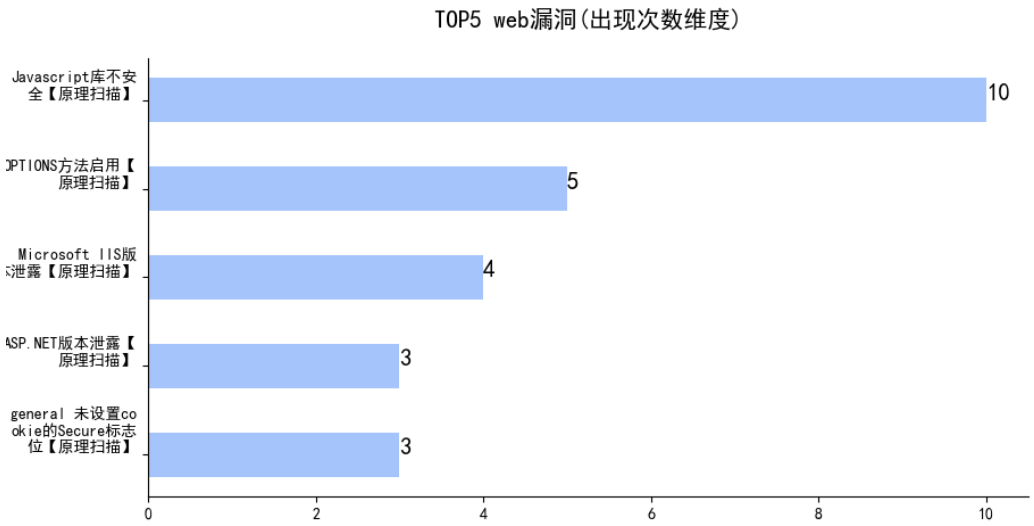
4.2.1 风险等级分析

4.2.2 影响资产分析

web漏洞影响资产数量TOP5统计如下：



出现次数指的是每个漏洞影响的端口或页面数量，web漏洞出现次数TOP５统计如下：



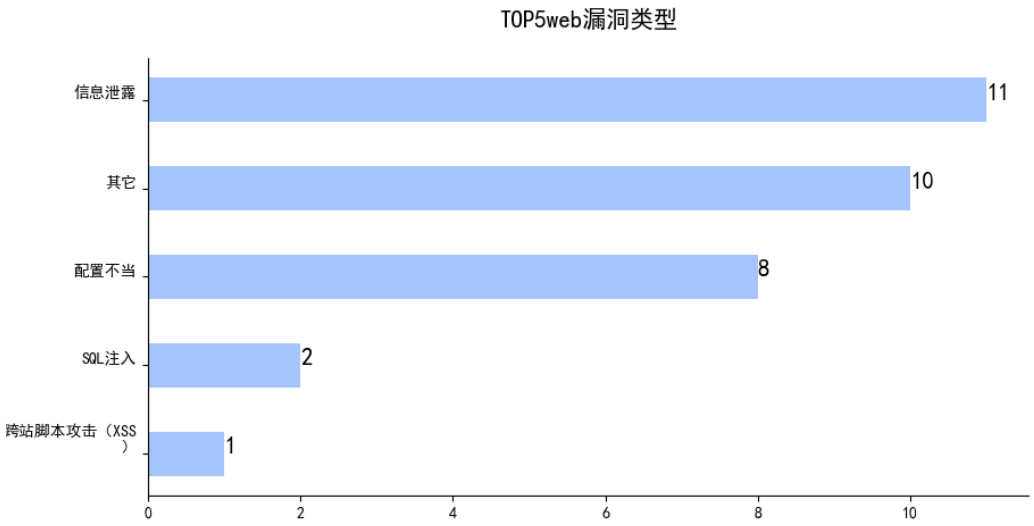
TOP100web漏洞影响资产情况如下表所示：

注：此处仅展示TOP100web漏洞及其影响资产情况，每个风险影响的资产最多展示10个，更多信息请登录平台查看，或者下载excel/html报告查看。

序号	web漏洞名称	风险等级	影响资产(仅展示10个)	影响资产数	出现次数
1	OPTIONS方法启用【原理扫描】	低	http://th-info.com http://www.th-storage.com http://byw3133480001.my3w.com http://th-storage.com http://www.th-info.com	5	5
2	Javascript库不安全【原理扫描】	中	http://th-info.com http://www.th-storage.com http://byw3133480001.my3w.com http://th-storage.com	4	10
3	Microsoft IIS版本泄露【原理扫描】	低	http://www.th-storage.com http://byw3133480001.my3w.com http://th-storage.com http://www.th-info.com	4	4
4	ASP.NET版本泄露【原理扫描】	低	http://www.th-storage.com http://th-storage.com http://www.th-info.com	3	3
5	general 未设置cookie的Secure标志位【原理扫描】	低	http://www.th-storage.com http://th-storage.com http://www.th-info.com	3	3
6	cookie 没有设置httponly标志位【原理扫描】	低	http://www.th-storage.com http://th-storage.com http://www.th-info.com	3	3
7	SQL注入攻击【原理扫描】	高	http://th-info.com http://www.th-storage.com	2	2
8	跨站脚本漏洞【原理扫描】	高	http://th-info.com	1	1
9	邮箱地址泄露【原理扫描】	低	http://www.th-storage.com	1	1

4.2.3 风险类型分析

web漏洞类别TOP５统计如下：



web漏洞类别TOP５统计如下：

序号	漏洞名称	出现次数
1	信息泄露	11
2	其它	10
3	配置不当	8
4	SQL注入	2
5	跨站脚本攻击（XSS）	1

4.3 弱口令影响分析

4.3.1 影响资产分析

未发现存在弱口令影响的资产。

4.4 登录入口影响分析

4.4.1 web登录入口影响资产分析

未发现存在web登录入口影响的资产。

4.4.2 系统登录入口影响资产分析

未发现存在系统登录入口影响的资产。

5 风险详情

5.1 http://th-storage.com

5.1.1 系统漏洞

1	IIS FastCGI请求头远程溢出漏洞(CVE-2010-2730)
风险等级	高
深信服漏洞编号	SF-0005-17607
CVE编号	CVE-2010-2730
CNNVD编号	CNNVD-201009-133
CNVD编号	CNVD-2010-2000
Bugtraq编号	43138
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。对于启用了FastCGI功能的IIS服务器，远程攻击者可以通过提交特制的HTTP请求触发缓冲区溢出，导致执行任意代码。
风险影响	影响IIS:7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS10-065）以及相应补丁 MS10-065：Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-065
风险举证	IIS:7.5

2	IIS FTPSVC远程拒绝服务漏洞(CVE-2010-3972)
风险等级	高
深信服漏洞编号	SF-0005-17606
CVE编号	CVE-2010-3972
CNNVD编号	CNNVD-201012-307
CNVD编号	
Bugtraq编号	45542
风险端口	80
	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。Windows 7 IIS 7.5处理请求中的Telnet协议转义

风险描述	时存在的堆溢出问题，远程可以利用此漏洞导致服务器程序崩溃，拒绝服务合法用户或导致执行任意代码。
风险影响	影响IIS:7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS11-004）以及相应补丁 MS11-004：Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-004
风险举证	IIS:7.5

3	IIS 重复参数请求拒绝服务漏洞(CVE-2010-1899)
风险等级	中
深信服漏洞编号	SF-0005-17608
CVE编号	CVE-2010-1899
CNNVD编号	CNNVD-201009-126
CNVD编号	CNVD-2010-1985
Bugtraq编号	43140
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。IIS中的脚本处理代码在处理重复的参数请求时存在栈溢出漏洞，远程攻击者可以通过对IIS所承载网站的ASP页面发送特制URI请求来利用这个漏洞，导致服务崩溃。
风险影响	影响IIS:6.0版本,7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS10-065）以及相应补丁 MS10-065：Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-065
风险举证	IIS:7.5

5.1.2 web漏洞

1	Javascript库不安全【原理扫描】
风险等级	中
深信服漏洞编号	SF-0000-0382
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80

风险描述	正在使用易受攻击的Javascript库。 已报告此版本的Javascript库存在一个或多个漏洞。 有关受影响的库和所报告的漏洞的更多信息，请查阅攻击详细信息和Web参考。
风险影响	有关更多信息，请参考Web参考。
解决方案	升级到最新版本。
风险举证	举证描述： Detected Javascript library jquery version 1.9.1. The version was detected from contents, and contents. 页面： http://th-storage.com/wei/jquery.js 请求： GET /wei/jquery.js HTTP/1.1 Cookie : ASPSESSIONIDQUACDRQR=DHKDHIOCKCKPIEMAGHHCPLGH; secure; path=/ User-Agent : Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 响应： HTTP/1.1 200 OK Content-Type : application/x-javascript Content-Encoding : gzip Last-Modified : Wed, 20 Sep 2017 06:04:10 GMT Accept-Ranges : bytes ETag : "0a98846d631d31:0" Vary : Accept-Encoding Server : Microsoft-IIS/7.5 Date : Wed, 19 Feb 2025 13:04:53 GMT Content-Length : 32837/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license */(function(e,t){var n,r,i=typeof t,o=e.document,a=e.location,s=e.jQuery,u=e.$,l={},c=[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,g=c.indexOf,m=l.toString,y=l.hasOwnProperty,v=p.trim,b=function(e,t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,w=/\S+/g,T=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:(<[\w\W]+>)[^>]*|#([\w-]*))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,k=/^[\],:{}\s]*$/,E=/(?:^|:|,)(?:\s*\[)+/g,S=/\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,A=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^-ms-/,D=/-([\da-z])/gi,L=function(e,t){return t.toUpperCase()},H=function(e){(o.addEventListener||"load"===e.type||"complete"===o.readyState)&&(q(),b.ready())},q=function(){o.addEventListener?(o.removeEventListener("DOMContentLoaded",H,!1),e.removeEventListener("load",H,!1)):(o.detachEvent("onreadystatechange",H),e.detachEvent("onload",H))};b.fn=b.prototype={jquery:p,constructor:b,init:function(e,n,r){var i,a;if(!e)return this;if("string"==typeof e){if(i="<"===e.charAt(0)&&">"===e.charAt(e.length-1)&&e.length>=3?[null,e,null]:N.exec(e),!i||!i[1]&&n)return!n||n.jquery?(n||r).find(e):this.constructor(n).find(e);if(i[1]){if(n=n instanceof b?n[0]:n,b.merge(this,b.parseHTML(i[1],n&&n.nodeType?n.ownerDocument||n:o,!0)),C.test(i[1])&&b.isPlainObject(n))for(i in n)b.isFunction(this[i])?this[i](n[i]):this.attr(i,n[i]);return this}if(a=o.getElementById(i[2]),a&&a.parentNode){if(a.id!==i[2])return r.find(e);this.length=1,this[0]=a}return this.context=o,this.selector=e,this}return e.nodeType?(this.context=this[0]=e,this.length=1,this):b.isFunction(e)?r.ready(e):(e.selector!==t&&(this.selector=e.selector,this.context=e.context),b.makeArray(e,this))},selector:"",length:0,size:function(){return this.length},toArray:function(){return h.call(this)},get:function(e){return null==e?this.toArray():0>e?this[this.length+e]:this[e]},pushStack:function(e){var t=b.merge(this.constructor(),e);return t.prevObject=this,t.context=this.context,t},each:function(e,t){return b.each(this,e,t)},ready:function(e){return b.ready.promise().done(e),this},slice:function(){return this.pushStack(h.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-1)},eq:function(e){var

	t=this.length,n=+e+(0>e?t:0);return this.pushStack(n>=0&&t>n?[this[n]]:[])},map:function(e){return this.pushStack(b.map(this,function(t,n){retur n e.call(t,n,t)}))},end:function(){return this.prevObject||this.constructor(null)},push:d,sort:[].sort,splice:[].s plice},b.fn.init.prototype=b.fn,b.extend=b.fn.extend=function(){var e,n,r,i,o,a,s=arguments[0]||
风险举证	{},u=1,l=arguments.length,c=!1;for("boolean"==typeof s&&(c=s,s=arguments[1]||{},u=2),"object"==typeof s||b.isFunction(s)||(s={}),l===u&&(s=this,--u);l>u;u++)if(null!=(o=argum ents[u]))for(i in o)e=s[i],r=o[i],s!==r&&(c&&r&&(b.isPlainObject(r)||(n= b.isArray(r)))?(n?(n=!1,a=e&&b.isArray(e)?e:[]):a=e&&b.isPlainObject(e)? e:{},s[i]=b.extend(c,a,r)):r!==t&&(s[i]=r));return s},b.extend({noConflict:function(t){return e.$===b&&(e.$=u),t&&e.jQuery===b&&(e.jQuery=s),b},isReady:!1,readyWait:1, holdReady:function(e){e?b.readyWait++:b.ready(!0)},ready:function(e){if(e===!0?!--b.readyWait:!b.isReady){if(!o.body)return setTimeout(b.ready);b.isReady=!0,e!==!0&&--b.readyWait>0||(n.resolveWith (o,[b]),b.fn.trigger&&b(o).trigger("ready").off("ready"))}},isFunction:f unction(e){return"function"===b.type(e)},isArray:Array.isArray||function (e){return"array"===b.type(e)},isWindow:function(e){return null!=e&&e==e.window},isNumeric:function(e){return!isNaN(parseFloat(e))& &isFinite(e)},type:function(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[m.call(e)]||"object":typeof e},isPlainObject:function(e){if(!e||"object"!==b.type(e)||e.nodeType||b. isWindow(e))return!1;try{if(e.constructor&&!y.call(e,"constructor")&&!y. call(e.constructor.prototype,"isPrototypeOf"))return!1}catch(n){return!1 }var r;for(r in e);return r===t||y.call(e,r)},isEmptyObject:function(e){ var t;for(t in e)return!1;return!0},error:function(e){throw Error(e)},parseHTML:function(e,t,n){if(!e||"string"!=typeof e)return null;"boolean"==typeof t&&(n=t,t=!1),t=t||o;var r=C.exec(e),i=!n&&[];return r?[t.createElement(r[1])]:(r=b.buildFragment ([e],t,i),i&&b(i).remove(),b.merge([],r.childNodes))},parseJSON:function

	(n){return e.JSON&&e.JSON.parse?e.JSON.parse(n):null===n?n:"string"==typeof n&&(n=b.trim(n),n&&k.test(n.replace(S,"@").replace(A,"]").replace(E," "))?Function("return "+n)():(b.error("Invalid JSON: "+n),t)},parseXML:function(n){var r,i;if(!n||"string"!=typeof n)return null;try{e.DOMParser?(i=new DOMParser,r=i.parseFromString(n,"text/xml")):(r=new ActiveXObject("Microsoft.XMLDOM"),r.async="false",r.loadXML(n))}catch(o){r=t}return r&&r.documentElement&&!r.getElementsByTagName("parsererror").length||b.error("Invalid XML: "+n),r},noop:function(){},globalEval:function(t){t&&b.trim(t)&&(e.execScript||function(t){e.eval.call(e,t)})(t)},camelCase:function(e){return e.replace(j,"ms-").replace(D,L)},nodeName:function(e,t){return e.nodeName&&e.nodeName.toLowerCase()===t.toLowerCase()},each:function(e,t,n){var r,i=0,o=e.length,a=M(e);if(n){if(a){for(;o>i;i++)if(r=t.apply(e[i],n),r===!1)break}else for(i in e)if(r=t.apply(e[i],n),r===!1)break}else if(a){for(;o>i;i++)if(r=t.call(e[i],i,e[i]),r===!1)break}else for(i in e)if(r=t.call(e[i],i,e[i]),r===!1)break;return e},trim:v&&!v.call("\ufeff\u00a0")?function(e){return null==e?"":v.call(e)}:function(e){return null==e?"":(e+"").replace(T,"")},makeArray:function(e,t){var n=t||[];return null!=e&&(M(Object(e))?b.merge(n,"string"==typeof e?[e]:e):d.call(n,e)),n},inArray:function(e,t,n){var r;if(t){if(g)return g.call(t,e,n);for(r=t.length,n=n?0>n?Math.max(0,r+n):n:0;r>n;n++)if(n in t&&t[n]===e)return n}return-1},merge:function(e,n){var r=n.length,i=e.length,o=0;if("number"==typeof r)for(;r>o
风险举证	;o++)e[i++]=n[o];else while(n[o]!==t)e[i++]=n[o++];return e.length=i,e},grep:function(e,t,n){var r,i=[],o=0,a=e.length;for(n=!!n;a>o;o++)r=!!t(e[o],o),n!==r&&i.push(e[o]);return i},map:function(e,t,n){var r,i=0,o=e.length,a=M(e),s=[];if(a)for(;o>i;i++)r=t(e[i],i,n),null!=r&&(s[s.length]=r);else for(i in e)r=t(e[i],i,n),null!=r&&(s[s.length]=r);return f.apply([],s)},guid:1,proxy:function(e,n){var r,i,o;return"string"==typeof n&&(o=e[n],n=e,e=o),b.isFunction(e)?(r=h.call(arguments,2),i=function(){return e.apply(n||this,r.concat(h.call(arguments)))},i.guid=e.guid=e.guid||b.guid++,i):t},access:function(e,n,r,i,o,a,s){var u=0,l=e.length,c=null==r;if("object"===b.type(r)){o=!0;for(u in r)b.access(e,n,u,r[u],!0,a,s)}else if(i!==t&&(o=!0,b.isFunction(i)||(s=!0),c&&(s?(n.call(e,i),n=null):(c=n,n=function(e,t,n){return c.call(b(e),n)})),n))for(;l>u;u++)n(e[u],r,s?i:i.call(e[u],u,n(e[u],r)));return o?e:c?n.call(e):l?n(e[0],r):a},now:function(){return(new Date).getTime()}}),b.ready.promise=function(t){if(!n)if(n=b.Deferred(),"complete"===o.readyState)setTimeout(b.ready);else if(o.addEventListener)o.addEventListener("DOMContentLoaded",H,!1),e.addEventListener("load",H,!1);else{o.attachEvent("onreadystatechange",H),e.attachEvent("onload",H);var r=!1;try{r=null==e.frameElement&&o.documentElement}catch(i){}r&&r.doScroll&&function a(){if(!b.isReady){try{r.doScroll("left")}catch(e){return setTimeout(a,50)}q(),b.ready()}}()}return n.promise(t)},b.each("Boolean Number String Function Array Date RegExp Object Error".split(" "),function(e,t){l["[object "+t+"]"]=t.toLowerCase()});function M(e){var t=e.length,n=b.type(e);return b.isWindow(e)?!1:1===e.nodeType&&t?!0:"array"===n||"function"!==n&&(0===t||"number"==typeof t&&t>0&&t-1 in

	e)}r=b(o);var _={};function F(e){var t=_[e]={};return b.each(e.match(w)||[],function(e,n){t[n]=!0}),t}b.Callbacks=function(e){ e="string"==typeof e?_[e]||F(e):b.extend({},e);var n,r,i,o,a,s,u=[],l=!e.once&&[],c=function(t){for(r=e.memory&&t,i=!0,a=s| |0,s=0,o=u.length,n=!0;u&&o>a;a++)if(u[a].apply(t[0],t[1])===!1&&e.stop O nFalse){r=!1;break}n=!1,u&&(l?l.length&&c(l.shift()):r?u=[]:p.disable()) },p={add:function(){if(u){var t=u.length;(function i(t){b.each(t,function(t,n){var r=b.type(n);"function"===r?e.unique&&p.h as(n)||u.push(n):n&&n.length&&"string"!==r&&i(n)})})(arguments),n?o=u.l e ngth:r&&(s=t,c(r))}return this},remove:function(){return u&&b.each(arguments,function(e,t){var r;while((r=b.inArray(t,u,r))>-1)u.splice(r,1),n&&(o>=r&&o--,a>=r&&a--)}), this},has:function(e){return e?b.inArray(e,u)>-1:!(!u||!u.length)},empt y: function(){return u=[],this},disable:function(){return u=l=r=t,this},disabled:function(){return!u},lock:function(){return l=t,r||p.disable(),this},locked:function(){return!l},fireWith:function(e, t){return t=t||[],t=[e,t.slice?t.slice():t],!u||i&&!l||(n?l.push(t):c(t)) ,this},fire:function(){return p.fireWith(this,arguments),this},fired:f un ction(){return!!i}};return p},b.extend({Deferred:function(e){var t=[["resolve","done",b.Callbacks("once memory"),"resolved"],["reject","fail",b.Callbacks("once memory"),"rejected"],["notif

2	Javascript库不安全【原理扫描】
风险等级	中
深信服漏洞编号	SF-0000-0382
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	正在使用易受攻击的Javascript库。 已报告此版本的Javascript库存在一个或多个漏洞。 有关受影响的库和所报告的漏洞的更多信息，请查阅攻击详细信息和Web参考。
风险影响	有关更多信息，请参考Web参考。
解决方案	升级到最新版本。
	举证描述： Detected Javascript library jquery-ui version 1.11.4. The version was detected from contents. 页面： http://th-storage.com/procss/main.js 请求： GET /procss/main.js HTTP/1.1 Cookie : ASPSESSIONIDQUACDRQR=DHKDHIOCKCKPIEMAGHHCPLGH; secure; path=/ User-Agent : Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 响应： HTTP/1.1 200 OK Content-Type : application/x-javascript Last-Modified : Wed, 20 Sep 2017 06:04:08 GMT Accept-Ranges : bytes ETag : "d1d57545d631d31:0" Server :

风险举证	Microsoft-IIS/7.5 Date : Wed, 19 Feb 2025 13:06:27 GMT Content-Length : 254577\xef\xbb\xbfvar mySwiper = null; var mySwiper2 = null; var mySwiper3 = null; var mySwiper4 = null; var mySwiper5 = null; var mySwiper7 = null; var mySwiper8 = null; var myScroll = null; var isPc = true; //\xe8\xbd\xae\xe6\x92\xad\xe5\x88\x9d\xe5\xa7\x8b\xe5\x8c\x96 function initSlides(){ $('.banner_show').css('display', 'block'); $('.rotate_pic').css('display', 'block'); if($('.swiper_1').children('div').children('div').length<=1){ mySwiper = new Swiper('.swiper_1',{ loop:false, autoplay:false, autoplayDisableOnInteraction:true, pagination : '.pagination1', createPagination :false, preventLinksPropagation : true, }); }else{ mySwiper = new Swiper('.swiper_1',{ loop:true, autoplay:8000, autoplayDisableOnInteraction:true, pagination : '.pagination1', createPagination :false, preventLinksPropagation : true, }); } $(".banner_show .arrow_r1").bind("click",function(){ mySwiper.swipeNext(); }); $(".banner_show . arrow_l1").bind("click",function(){ mySwiper.swipePrev(); }); if (isPc){ $(".pagination1 li a").each(function(index,el){ $(el).bind("click",function(){ mySwiper.stopAutoplay(); mySwiper.swipeTo(index); mySwiper.startAutoplay(); }) }) }else{ $(".pagination1 li a").each(function(index,el){ $(el).bind("touchend " , function(){ mySwiper.stopAutoplay(); mySwiper.swipeTo(index); mySwiper.startAutoplay(); }) }) } // mySwiper.stopAutoplay(); if($('.swiper_2').length>0){ mySwiper2 = new Swiper('.swiper_2',{ autoplayDisableOnInteraction:false, createPagination :false, preventLinksPropagation : true, slidesPerView : "auto", }); $(".showProduct .arrow_r").bind("click",function(){ mySwiper2.swipeNext(); }); $(".showProduct . arrow_l").bind("click",function(){ mySwiper2.swipePrev(); }); } if($('.swiper_3').length>0){ mySwiper3 = new Swiper('.swiper_3',{ autoplayDisableOnInteraction:false, createPagination :false, preventLinksPropagation : true, slidesPerView : 1, }); $(".information . arrow_l2").bind("click",function(){ mySwiper3.swipeNext(); }); $(".information .arrow_r2").bind("click",function(){ mySwiper3.swipePrev(); }); $(".information_sp . arrowL").bind("click",function(){ mySwiper3.swipePrev(); }); $(".information_sp .arrowR").bind("click",function(){ mySwiper3.swipeNext(); }); $(".information_sp . arrow_r2").bind("click",function(){ mySwiper3.swipePrev(); }); $(".information_sp .arrow_l2").bind("click",function(){ mySwiper3.swipeNext(); }); } if($('.swiper_4').length>0){ mySwiper4 = new Swiper('.swiper_4',{ aut
	oplayDisableOnInteraction:false, createPagination :false, preventLinksPropagation : true, slidesPerView : 4, }); $(".nav").on("click",".arrow_l",function(){ mySwiper4.swipePrev(); }); $(".nav").on("click",".arrow_r",function(){ mySwiper4.swipeNext(); }); } if($('.swiper_5').length>0){ mySwiper5 = new Swiper('.swiper_5',{ autoplayDisableOnInteraction:false, createPagination :false, preventLinksPropagation : true, slidesPerView : 4, }); $(".nav").on("click",".swiper_5_l",function(){ mySwiper5.swipePrev(); }); $(".nav").on("click",".swiper_5_r",function(){ mySwiper5.swipeNext(); }); } /*mySwiper6 = new Swiper('.swiper_6',{ autoplayDisableOnInteraction:false, createPagination :false,

风险举证	preventLinksPropagation : true, slidesPerView : 4, }); */ if($('.swiper_7').length>0){ if($('.swiper_7').children('div').children(' div').length<=1){ mySwiper7 = new Swiper('.swiper_7',{ loop:false, autoplay:false, autoplayDisableOnInteraction:true, pagination : ' . pagination7', createPagination :false, preventLinksPropagation : true, }); }else{ mySwiper7 = new Swiper('.swiper_7',{ loop:true, autoplay:3600, autoplayDisableOnInteraction:true, pagination : ' . pagination7', createPagination :false, preventLinksPropagation : true, }); } if (isPc){ $(".pagination7 li a").each(function(index,el){ $(el).bind("click",function(){ mySwiper7.stopAutoplay(); mySwiper7.swipeTo(index); mySwiper7.startAutoplay(); }) }) }else{ $(".pagination7 li a").each(function(index,el){ $(el).bind("touchend " , function(){ mySwiper7.stopAutoplay(); mySwiper7.swipeTo(index); mySwiper7.startAutoplay(); }) }) } mySwiper7.stopAutoplay(); $(".arrow_r7").bind("click",function(){ mySwiper7.swipeNext(); }); $(".arrow_l7").bind("click",function(){ mySwiper7.swipePrev(); }); } //8 if($('.swiper_8').length>0){ mySwiper8 = new Swiper('.swiper_8',{ loop:true, autoplay:3600, autoplayDisableOnInteraction:true, createPagination :false, preventLinksPropagation : true, }); mySwiper8.stopAutoplay(); $(".arrow_r8").bind("click",function(){ mySwiper8.swipeNext(); }); $(".arrow_l8").bind("click",function(){ mySwiper8.swipePrev(); }); } $(".swiper-wrapper").height("auto"); $(".swiper-slide").height("auto"); $(".swiper_3,.swiper_3 . swiper-wrapper,.swiper_3 .swiper-wrapper . swiper-slide").height("100%"); } function scrollBody(){ var uaString = navigator.userAgent.toLowerCase(); if (uaString.indexOf('android') < 0 && uaString.indexOf('iphone') < 0 && uaString.indexOf('ipad') < 0 && uaString.indexOf('tablet') < 0){ } else{ /*$(".container").css("overflow","hidden"); myScroll = new IScroll('.container', {hScroll:false,bounce:false,vScrollbar:false}); myScroll._resize();*/ } } function initEvent(){ $(".m_nav . showNav").unbind().bind("touchend",function(){ if (!$(".menu_push").hasClass("menu_push_open")){ $(".menu_push").addClass("menu_push_open").stop(true,true).slideDown(); $(".showNav_img").attr("src", "/common/Style/img/nav_close.png"); } else{ $
	(".menu_push").removeClass("menu_push_open").stop(true,true).slideUp(); $(".showNav_img").attr("src", "/common/Style/img/nav.png"); } }); $(".m_menu_1").on("touchend","li",function(){ var _this = $(this); if (_this.hasClass("active")) return; else { $(".m_menu_1 li.active").removeClass("active"); _this.addClass("active"); /*var currIndex = function () { var _index; $(".m_menu_1 li").each(function(index, el) { console.log($(_this)); console.log($(el)); if ($(_this) == $(el)) { _index = index; } }); return _index; } console.log(currIndex());*/ } }); $(".sosoM").unbind().bind("click",function(){ if (!$(".soso_push_m").hasClass("soso_push_open")){ $(".soso_push_m").addClass("soso_push_open").stop(true,true).slideDown(); } else{ $(".soso_push_m").removeClass("soso_push_open").stop(true,true).slideUp(); } }); //\xe7\x82\xb9\xe5\x87\xbb\xe5\x88\xab\xe5\xa4\x84 \xe6\x94\xb6\xe7\xb4\xa2\xe6\xa1\x86\xe6\x94\xb6\xe8\xb5\xb7 $(document).unbind().bind("touchend","touchmove", function(){ var eo = $(event.target); if (eo.parent().attr("class") != "sosoM" && !

风险举证	eo.parent(".m_nav").length && !eo.parent(".soso_push_m").length && eo.attr("class") != "soso_push_m") { $(".soso_push_m").removeClass("soso _push_open").stop(true,true).slideUp(); } }) $(".soso_close").unbind().bind("click",function(){ location.href = " /Apps/search/index.aspx?key=" + $('#searchProducts_all').val(); }); } function isMobile(){ var uaString = navigator.userAgent.toLowerCase(); if (uaString.indexOf('android') < 0 && uaString.indexOf('iphone') < 0 && uaString.indexOf('ipad') < 0 && uaString.indexOf('tablet') < 0){ isPc = true; } else{ isPc = false; } } $(function(){ $('.rotate_pic_cx').css('height', '0px').css('overflow','hidden') isMobile(); if (isPc) { $("#searchProducts_form").css('display', ' none'); } $(window).resizeEnd({ delay : 0 }, function() { //console.log(mySwiper) if($('.swiper_1').length>0){ if (mySwiper) { mySwiper.resizeFix(); //$('.banner_show').css('height', $(".swiper_1").height() + 'px'); } } if($('.swiper_2').length>0){ if (mySwiper2) mySwiper2.resizeFix(); } if($('.swiper_3').length>0){ if (mySwiper3) mySwiper3.resizeFix(); } if($('.swiper_4').length>0){ if (mySwiper4) mySwiper4.resizeFix(); } if($('.swiper_5').length>0){ if (mySwiper5) mySwiper5.resizeFix(); } if($('.swiper_7').length>0){ if (mySwiper7) { mySwiper7.resizeFix(); //$('.rotate_pic').css('height', $(".s

3	Javascript库不安全【原理扫描】
风险等级	中
深信服漏洞编号	SF-0000-0382
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	正在使用易受攻击的Javascript库。 已报告此版本的Javascript库存在一个或多个漏洞。 有关受影响的库和所报告的漏洞的更多信息，请查阅攻击详细信息和Web参考。
风险影响	有关更多信息，请参考Web参考。
解决方案	升级到最新版本。
	举证描述： Detected Javascript library jquery-ui version 1.11.4. The version was detected from contents. 页面： http://th-storage.com/indexcss/jquery-ui.js 请求： GET /indexcss/jquery-ui.js HTTP/1.1 Cookie : ASPSESSIONIDQUACDRQR=DHKDHIOCKCKPIEMAGHHCPLGH; secure; path=/ User-Agent : Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 响应： HTTP/1.1 200 OK Content-Type : application/x-javascript Last-Modified : Wed, 20 Sep 2017 06:04:03 GMT Accept-Ranges : bytes ETag : "61597142d631d31:0" Server : Microsoft-IIS/7.5 Date : Wed, 19 Feb 2025 13:07:56 GMT Content-Length : 240434\xef\xbb\xbf/*! jQuery UI - v1.11.4 - 2015-03-11 * http://jqueryui.com * Includes: core.js, widget.js, mouse.js,

风险举证	position.js, accordion.js, autocomplete.js, button.js, datepicker.js, dialog.js, draggable.js, droppable.js, effect.js, effect-blind.js, effect-bounce.js, effect-clip.js, effect-drop.js, effect-explode.js, effect-fade.js, effect-fold.js, effect-highlight.js, effect-puff.js, effect-pulsate.js, effect-scale.js, effect-shake.js, effect-size.js, effect-slide.js, effect-transfer.js, menu.js, progressbar.js, resizable.js, selectable.js, selectmenu.js, slider.js, sortable.js, spinner.js, tabs.js, tooltip.js * Copyright 2015 jQuery Foundation and other contributors; Licensed MIT */ (function(e){"function"==typeof define&&define.amd?define(["jquery"],e):e(jQuery)})(function(e){function t(t,s){var n,a,o,r=t.nodeName.toLowerCase();return"area"===r?(n=t.parent tNode,a=n.name,t.href&&a&&"map"===n.nodeName.toLowerCase()?(o=e("img[use map='#"+a+"']")[0],!!o&&i(o)):!1):(/^(input|select|textarea|button|objec t)$/.test(r)?!t.disabled:"a"===r?t.href||s:s)&&i(t)}function i(t){return e.expr.filters.visible(t)&&!e(t).parents().addBack().filter(function(){return"hidden"===e.css(this,"visibility")}).length}function s(e){for(var t,i;e.length&&e[0]!==document;){if(t=e.css("position"),("ab solute"===t||"relative"===t||"fixed"===t)&&(i=parseInt(e.css("zIndex"), 1 0),!isNaN(i)&&0!==i))return i;e=e.parent()}return 0}function n(){this._curInst=null,this._keyEvent=!1,this._disabledInputs=[],this._d atepickerShowing=!1,this._inDialog=!1,this._mainDivId="ui-datepicker-div" ,this._inlineClass="ui-datepicker-inline",this._appendClass="ui-datepick er-append",this._triggerClass="ui-datepicker-trigger",this._dialogCl ass=" ui-datepicker-dialog",this._disableClass="ui-datepicker-disabled", this._ unselectableClass="ui-datepicker-unselectable",this._currentClass ="ui-da tepicker-current-day",this._dayOverClass="ui-datepicker-days-cel l-over", this.regional=[],this.regional[""]={closeText:"Done",prevText:" Prev",nex tText:"Next",currentText:"Today",monthNames:["January","Februa ry","March" ,"April","May","June","July","August","September","October","N ovember"," December"],monthNamesShort:["Jan","Feb","Mar","Apr","May","J un","Jul","A ug","Sep","Oct","Nov","Dec"],dayNames:["Sunday","Monday","T uesday","Wedn esday","Thursday","Friday","Saturday"],dayNamesShort:["Sun" ,"Mon","Tue"," Wed","Thu","Fri","Sat"],dayNamesMin:["Su","Mo","Tu","We","T h","Fr","Sa"], weekHeader:"Wk",dateFormat:"mm/dd/yy",firstDay:0,isRTL:! 1,showMonthAfter Year:!1,yearSuffix:""},this._defaults={showOn:"focus",s howAnim:"fadeIn", showOptions:{},defaultDate:null,appendText:"",buttonTe xt:"...",buttonIma ge:"",buttonImageOnly:!1,hideIfNoPrevNext:!1,navigati onAsDateFormat:!1,g otoCurrent:!1,changeMonth:!1,cha
	ngeYear:!1,yearRange:"c-10:c+10",showOtherMonths:!1,selectOtherMonths:!1, showWeek:!1,calculateWeek:this.iso8601Week,shortYearCutoff:"+10",minDate: null,maxDate:null,duration:"fast",beforeShowDay:null,beforeShow:null,onS elect:null,onChangeMonthYear:null,onClose:null,numberOfMonths:1,showCurr entAtPos:0,stepMonths:1,stepBigMonths:12,altField:"",altFormat:"",constr ainInput:!0,showButtonPanel:!1,autoSize:!1,disabled:!1},e.extend(this._d efaults,this.regional[""]),this.regional.en=e.extend(!0,{},this.regional [""]),this.regional["en-US"]=e.extend(!0,{},this.regional.en),this.dpDiv =a(e(" "))}function a(t){var i="button, .ui-datepicker-prev, .ui-datepicker-next, . ui-datepicker-calendar td a";return t.delegate(i,"mouseout",function(){e (this).removeClass("ui-state-hover"),-1!==this.className.indexOf("ui-dat epicker-prev")&&e(this).removeClass("ui-datepicker-prev-hover"),-1!==thi s.className.indexOf("ui-datepicker-next")&&e(this).removeClass("ui-datep

风险举证	icker-next-hover")}).delegate(i,"mouseover",o)}function o(){e.datepicker._isDisabledDatepicker(v.inline?v.dpDiv.parent()[0]:v.input[0])||(e(this).parents(".ui-datepicker-calendar").find("a").removeClass("ui-state-hover"),e(this).addClass("ui-state-hover"),-1!==this.className.indexOf("ui-datepicker-prev")&&e(this).addClass("ui-datepicker-prev- hover"),-1!==this.className.indexOf("ui-datepicker-next")&&e(this).addCl ass("ui-datepicker-next-hover"))}function r(t,i){e.extend(t,i);for(var s in i)null==i[s]&&(t[s]=i[s]);return t}function h(e){return function(){var t=this.element.val();e.apply(this,arguments),this._refresh(),t!==this.element.val()&&this._trigger("change")}}e.ui=e.ui||{},e.extend(e.ui,{version:"1.11.4",keyCode:{BACKSPACE:8,COMMA:188,DELETE:46,DOWN: 40,END:35,ENTER:13,ESCAPE:27,HOME:36,LEFT:37,PAGE_DOWN:34,PAGE_UP:33,PERIOD:190,RIGHT:39,SPACE:32,TAB:9,UP:38}}),e.fn.extend({scrollParent:function(t){var i=this.css("position"),s="absolute"===i,n=t?/(auto|scroll|hidden)/:/(auto|scroll)/,a=this.parents().filter(function(){var t=e(this);return s&&"static"===t.css("position")?!1:n.test(t.css("overflow")+t.css("overflow-y")+t.css("overflow-x"))}).eq(0);return"fixed"!==i&& a.length?a:e(this[0].ownerDocument||document)},uniqueId:function(){var e=0;return function(){return this.each(function(){this.id||(this.id="ui- id-"+ ++e)})}}(),removeUniqueId:function(){return this.each(function(){/^ui-id-\d+$/.test(this.id)&&e(this).removeAttr("id")})}}),e.extend(e.expr[":"],{data:e.expr.createPseudo?e.expr.createPseudo(function(t){return function(i){return!!e.data(i,t)}}):function(t,i,s){return!!e.data(t,s[3])},focusable:function(i){return t(i,!isNaN(e.attr(i,"tabindex")))},tabbable:function(i){var s=e.attr(i,"tabindex"),n=isNaN(s);return(n||s>=0)&&t(i,!n)}}),e("<a>").outerWidth(1).jquery||e.each(["Width","Height"],function(t,i){function s(t,i,s,a){return e.each(n,function(){i-=parseFloat(e.css(t,"padding"+this))||0,s&&(i-=parseFloat(e.css(t,"border"+this+"Width"))||0),a&&(i-=parseFloat(e.css(t,"margin"+this))||0)}),i}var n="Width"===i?["Left","Right"]:["Top","Bottom"],a=i.toLowerCase(),o={innerWidth:e.fn.innerWidth,innerHeight:e.fn.innerHeight,outerWidth:e.fn.outerWidth,outerHeight:e.fn.outerHeight};e.fn["inner"+i]=function(t){return void 0===t?o["inner"+i].call(this):this.each(function(){e(this).css(a,s(this,t)+"px")})},e.fn["outer"+i]=function(t,n){return"number"!=typeof t?o["outer"+i].call(this,t):this.each(function(){e(this).css(a,s(this,t,!0,n)+"px")})}}),e.fn.addBack||(e.fn.addBack=function(e){return this.add(null==e?this.prevObject:this.prevObject.filter(e))}),e("<a>").data("a-b","a").removeData("a-b").data("a-b")&&(e.fn.removeData=function(t){return function(i){return arguments.length?t.call(this,e.camelCase(i)):t.call(this)}}(e.fn.removeData)),e.ui.ie=!!/msie [\w.]+/.exec(navigator.userAgent.toLowerCase()),e.fn.extend({focus:function(t){return function(i,s){return"number"==typeof i?this.each(function(){var t=this;setTimeout(function(){e(t).focus(),s&&s.call(t)},i)}):t.apply(this,arguments)}}(e.fn.focus),disableSelection:function(){var e="onselectstart"in document.createElement("div")?"selectstart":"mousedown";return function(){return this.bind(e+".ui-disableSelection",function(e){e.preventDefault()})}}(),enableSelection:function(){return this.unbind(".ui-disableSelection")},zIndex:function(t){if(void 0!==t)return this.css("zIndex",t);if(this.length)for(var i,s,n=e(this[0]);n.length&&n[0]!==document;){if(i=n.css("position"),("ab
	his).css(a,s(this,t)+"px")})},e.fn["outer"+i]=function(t,n){return"number"!=typeof t?o["outer"+i].call(this,t):this.each(function(){e(this).css(a,s(this,t,!0,n)+"px")})}}),e.fn.addBack||(e.fn.addBack=function(e){return this.add(null==e?this.prevObject:this.prevObject.filter(e))}),e("<a>").data("a-b","a").removeData("a-b").data("a-b")&&(e.fn.removeData=function(t){return function(i){return arguments.length?t.call(this,e.camelCase(i)):t.call(this)}}(e.fn.removeData)),e.ui.ie=!!/msie [\w.]+/.exec(navigator.userAgent.toLowerCase()),e.fn.extend({focus:function(t){return function(i,s){return"number"==typeof i?this.each(function(){var t=this;setTimeout(function(){e(t).focus(),s&&s.call(t)},i)}):t.apply(this,arguments)}}(e.fn.focus),disableSelection:function(){var e="onselectstart"in document.createElement("div")?"selectstart":"mousedown";return function(){return this.bind(e+".ui-disableSelection",function(e){e.preventDefault()})}}(),enableSelection:function(){return this.unbind(".ui-disableSelection")},zIndex:function(t){if(void 0!==t)return this.css("zIndex",t);if(this.length)for(var i,s,n=e(this[0]);n.length&&n[0]!==document;){if(i=n.css("position"),("ab

风险举证	solute"===i||"relative"===i||"fixed"===i)&&(s=parseInt(n.css("zIndex"),10),!isNaN(s)&&0!==s))return s;n=n.parent()}return 0}}),e.ui.plugin={add:function(t,i,s){var n,a=e.ui[t].prototype;for(n in s)a.plugins[n]=a.plugins[n]||[],a.plugins[n].push([i,s[n]])},call:function(e,t,i,s){var n,a=e.plugins[t];if(a&&(s||e.element[0].parentNode&&11!==e.element[0].parentNode.nodeType))for(n=0;a.length>n;n++)e.options[a[n][0]]&&a[n][1].apply(e.element,i)}};var l=0,u=Array.prototype.slice;e.cleanData=function(t){return function(i){var s,n,a;for(a=0;null!=(n=i[a]);a++)try{s=e._data(n,"events"),s&&s.remove&&e(n).triggerHandler("remove")}catch(o){}t(i)}}(e.cleanData),e.widget=function(t,i,s){var n,a,o,r,h={},l=t.split(".")[0];return t=t.split(".")[1],n=l+"-"+t,s||(s=i,i=e.Widget),e.expr[":"][n.toLowerCase()]=function(t){return!!e.data(t,n)},e[l]=e[l]||{},a=e[l][t],o=e[l][t]=function(e,t){return this._createWidget?(arguments.length&&this._createW idget(e,t),void 0):new o(e,t)},e.extend(o,a,{version:s.version,_proto:e.extend({},s),_childConstructors:[]}),r=new i,r.options=e.widget.extend({},r.options),e.each(s,function(t,s){return e.isFunction(s)?(h[t]=function(){var e=function(){return i.prototype[t].apply(this,arguments)},n=function(e){return i.prototype[t].apply(this,e)};return function(){var t,i=this._super,a=this._superApply;return this._super=e,this._superApply=n,t=s.apply(this,arguments),this._super=i,this._superApply=a,t}}(),void 0):(h[t]=s,void 0)}),o.prototype=e.widget.extend(r,{widgetEventPrefix:a?r.widgetEventPrefix||t:t},h,{constructor:o,namespace:l,widgetName:t,widgetFullName:n}),a?(e.each(a._childConstructors,function(t,i){var s=i.prototype;e.widget(s.namespace+"."+s

4	Javascript库不安全【原理扫描】
风险等级	中
深信服漏洞编号	SF-0000-0382
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	正在使用易受攻击的Javascript库。 已报告此版本的Javascript库存在一个或多个漏洞。 有关受影响的库和所报告的漏洞的更多信息，请查阅攻击详细信息和Web参考。
风险影响	有关更多信息，请参考Web参考。
解决方案	升级到最新版本。
	举证描述： Detected Javascript library jquery version 1.4.2. The version was detected from name, and contents, and contents. 页面： http://th-storage.com//pro/jquery-1.4.2.js 请求： GET //pro/jquery-1.4.2.js HTTP/1.1 Cookie : ASPSESSIONIDQUACDRQR=DHKDHIOCKCKPIEMAGHHCPLGH; secure; path=/ Referer : http://th-storage.com//about30/css/404.css User-Agent : Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

风险举证	Chrome/80.0.3987.132 Safari/537.36 响应： HTTP/1.1 200 OK Content-Type : application/x-javascript Last-Modified : Mon, 31 Oct 2016 12:48:34 GMT Accept-Ranges : bytes ETag : "bd8e4e177533d21:0" Server : Microsoft-IIS/7.5 Date : Wed, 19 Feb 2025 13:51:49 GMT Content-Length : 170093/*! * jQuery JavaScript Library v1.4.2 * http://jquery.com/ * * Copyright 2010, John Resig * Dual licensed under the MIT or GPL Version 2 licenses. * http://jquery.org/license * * Includes Sizzle.js * http://sizzlejs.com/ * Copyright 2010, The Dojo Foundation * Released under the MIT, BSD, and GPL Licenses. * * Date: Sat Feb 13 22:33:48 2010 -0500 */ (function(window, undefined) { // Define a local copy of jQuery var jQuery = function(selector, context) { // The jQuery object is actually just the init constructor 'enhanced' return new jQuery.fn.init(selector, context); }, // Map over jQuery in case of overwrite _jQuery = window.jQuery, // Map over the $ in case of overwrite _$ = window.$, // Use the correct document accordingly with window argument (sandbox) document = window.document, // A central reference to the root jQuery(document) rootjQuery, // A simple way to check for HTML strings or ID strings // (both of which we optimize for) quickExpr = /^[^<]*(<[\w\W]+>)[^>]*$|^#([\w-]+)$/, // Is it a simple selector isSimple = /^.[^:#\[\.,]*$/, // Check if a string has a non-whitespace character in it rnotwhite = /\S/, // Used for trimming whitespace rtrim = /^(\s|\u00A0)+|(\s|\u00A0)+$/g, // Match a standalone tag rsingleTag = /^<(\w+)\s*\/?>(?:<\/\1>)?$/, // Keep a UserAgent string for use with jQuery.browser userAgent = navigator.userAgent, // For matching the engine and version of the browser browserMatch, // Has the ready events already been bound? readyBound = false, // The functions to execute on DOM ready readyList = [], // The ready event handler DOMContentLoaded, // Save a reference to some core methods toString = Object.prototype.toString, hasOwnProperty = Object.prototype.hasOwnProperty, push = Array.prototype.push, slice = Array.prototype.slice, indexOf = Array.prototype.indexOf; jQuery.fn = jQuery.prototype = { init: function(selector, context) { var match, elem, ret, doc; // Handle $(""), $(null), or $(undefined) if (!selector) { return this; } // Handle $(DOMElement) if (selector.nodeType) { this.context = this[0] = selector; this.length = 1; return this; } // The body element only exists once, optimize finding it if (selector === "body" && !context) { this.context = document; this[0] = document.body; this.selector = "body"; this.length = 1; return this; } // Handle HTML strings if (typeof selector === "string") { // Are we dealing with HTML string or an ID? match = quickExpr.exec(selector); // Verify a matc
	h, and that no context was specified for #id if (match && (match[1] || !context)) { // HANDLE: $(html) -> $(array) if (match[1]) { doc = (context ? context.ownerDocument || context : document); // If a single string is passed in and it's a single tag // just do a createElement and skip the rest ret = rsingleTag.exec(selector); if (ret) { if (jQuery.isPlainObject(context)) { selector = [document.createElement(ret[1])]; jQuery.fn.attr.call(selector, context, true); } else { selector = [doc.createElement(ret[1])]; } } else { ret = buildFragment([match[1]], [doc]); selector = (ret.cacheable ? ret.fragment.cloneNode(true) : ret.fragment).childNodes; } return jQuery.merge(this, selector); // HANDLE: $("#id") } else { elem = document.getElementById(match[2]);

风险举证	if (elem) { // Handle the case where IE and Opera return items // by name instead of ID if (elem.id !== match[2]) { return rootjQuery.find(selector); } // Otherwise, we inject the element directly into the jQuery object this.length = 1; this[0] = elem; } this.context = document; this.selector = selector; return this; } // HANDLE: $("TAG") } else if (!context && /^\w+$/.test(selector)) { this.selector = selector; this.context = document; selector = document.getElementsByTagName(selector); return jQuery.merge(this, selector); // HANDLE: $(expr, $(...)) } else if (!context || context.jquery) { return (context || rootjQuery).find(selector); // HANDLE: $(expr, context) // (which is just equivalent to: $(context).find(expr) } else { return jQuery(context).find(selector) ; } // HANDLE: $(function) // Shortcut for document ready } else if (jQuery.isFunction(selector)) { return rootjQuery.ready(selector); } if (selector.selector !== undefined) { this.selector = selector.selector; this.context = selector.context; } return jQuery.makeArray(selector, this); }, // Start with an empty selector selector: "", // The current version of jQuery being used jquery: " 1.4.2", // The default length of a jQuery object is 0 length: 0, // The number of elements contained in the matched element set size: function() { return this.length; }, toArray: function() { return slice.call(this, 0); }, // Get the Nth element in the matched element set OR // Get the whole matched element set as a clean array get: function(num) { return num == null ? // Return a 'clean' array this.toArray() : // Return just the object (num < 0 ? this.slice(num)[0] : this[num]); }, // Take an array of elements and push it onto the stack // (returning the new matched element set) pushStack: function(elems, name, selector) { // Build a new jQuery matched element set var ret = jQuery(); if (jQuery.isArray(elems)) { push.apply(ret, elems); } else { jQuery.merge(ret, elems); } // Add the old object onto the stack (as a reference) ret.prevObject = this; ret.context = this.context; if (name === "find") { ret.selector = this.selector + (this.selector ? " " : "")
风险举证	+ selector; } else if (name) { ret.selector = this.selector + "." + name + "(" + selector + ")"; } // Return the newly-formed element set return ret; }, // Execute a callback for every element in the matched set. // (You can seed the arguments with an array of args, but this is // only used internally.) each: function(callback, args) { return jQuery.each(this, callback, args); }, ready: function(fn) { // Attach the listeners jQuery.bindReady(); // If the DOM is already ready if (jQuery.isReady) { // Execute the function immediately fn.call(document, jQuery); // Otherwise, remember the function for later } else if (readyList) { // Add the function to the wait list readyList.push(fn); } return this; }, eq: function(i) { return i === -1 ? this.slice(i) : this.slice(i, +i + 1); }, first: function() { return this.eq(0); }, last: function() { return this.eq(-1); }, slice: function() { return this.pushStack(slice.apply(this, arguments), "slice", slice.call(arguments).join(",")); }, map: function(callback) { return this.pushStack(jQuery.map(this, function(elem, i) { return callback.call(elem, i, elem); })); }, end: function() { return this.prevObject || jQuery(null); }, // For internal use only. // Behaves like an Array's method, not like a jQuery method. push: push, sort: [].sort, splice: [].splice }; // Give the

	init function the jQuery prototype for later instantiation jQuery.fn.init.prototype = jQuery.fn; jQuery.extend = jQuery.fn.extend = function() { // copy reference to target object var target = arguments[0] || {}, i = 1, length = arguments.length, deep = false, options, name, src, copy; // Handle a deep copy situation if (typeof target === "boolean") { deep = target; target = arguments[1] || {}; // skip the boolean and the target i = 2; } // Handle case when target is a string or something (possible in deep copy) if (typeof target !== "object" && !jQuery.isFunction(target)) { target = {}; } // extend jQuery itself if only one argument is passed if (length === i) { target = this; --i; } for (; i < length; i++) { // Only deal with non-null/undefined values if ((options = arguments[i]) != null) { // Extend the base object for (name in options) { src = target[name] ; copy = options[name]; // Prevent never-ending loop if (target === copy) { continue; } // Recurse if we're merging object literal values or arrays if (deep && copy && (jQuery.isPlainObject(copy) || jQuery.isArray(copy))) { var clone

5	Javascript库不安全【原理扫描】
风险等级	中
深信服漏洞编号	SF-0000-0382
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	正在使用易受攻击的Javascript库。 已报告此版本的Javascript库存在一个或多个漏洞。 有关受影响的库和所报告的漏洞的更多信息，请查阅攻击详细信息和Web参考。
风险影响	有关更多信息，请参考Web参考。
解决方案	升级到最新版本。
	举证描述： Detected Javascript library jquery version 1.9.1. The version was detected from contents, and contents. 页面： http://th-storage.com/wei/jQuery.js 请求： GET /wei/jQuery.js HTTP/1.1 Accept : */* Cookie : Hm_lvt_597805b8f3a912caaa0e90184d25abc0=1739969897; Hm_lpvt_597805b8f3a912caaa0e90184d25abc0=1739969897; HMACCOUNT=9CC6680E0D2F420C; sajssdk_2015_cross_new_user=1; sensorsdata2015jssdkcross=%7B%22distinct_id%22%3A%221951e49b9ab9ea-0c11facd8098d4-26021a51-921600-1951e49b9b232f%22%2C%22first_id%22%3A%22%22%2C%22props%22%3A%7B%22%24latest_traffic_source_type%22%3A%22%E7%9B%B4%E6%8E%A5%E6%B5%81%E9%87%8F%22%2C%22%24latest_search_keyword%22%3A%22%E6%9C%AA%E5%8F%96%E5%88%B0%E5%80%BC_%E7%9B%B4%E6%8E%A5%E6%89%93%E5%BC%80%22%2C%22%24latest_referrer%22%3A%22%22%7D%2C%22identities%22%3A%22eyIkaWRlbnRpdHlfY29va2llX2lkIjoiMTk1MWU0OWI5YWI5ZWEtMGMxMWZhY2Q4MDk4ZDQtMjYwMjFhNTEtOTIxNjAwLTE5NTFlNDliOWIyMzJmIn0%3D%22%2C%22history_login_id%22%3A%7B%22name%22%3A%22%22%2C%22value%22%3A%22%22%7D%2C%22%24device_id%22%3A%221951

风险举证	e49b9ab9ea-0c11facd8098d4-26021a51-921600-1951e49b9b232f%22%7D; __bid_n=1951e49ba374944991ebd8; ASPSESSIONIDQQACDRQR=IIKDHIOCBMLBPBGKBEA GONJK Referer : http://th-storage.com/service.asp?cataid=24 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36 响应： HTTP/1.1 200 OK Content-Type : application/x-javascript Content-Encoding : gzip Last-Modified : Wed, 20 Sep 2017 06:04:10 GMT Accept-Ranges : bytes ETag : "0a98846d631d31:0" Vary : Accept-Encoding Server : Microsoft-IIS/7.5 Date : Wed, 19 Feb 2025 13:04:11 GMT Content-Length : 32837/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license */(function(e,t){var n,r,i=typeof t,o=e.document,a=e.location,s=e.jQuery,u=e.$,l={},c=[],p="1.9.1",f=c.con cat,d=c.push,h=c.slice,g=c.indexOf,m=l.toString,y=l.hasOwnProperty,v=p.t rim,b=function(e,t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.\|)\d+(?: [eE][+-]?\d+\|)/.source,w=/\S+/g,T=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N =/^(?:(<[\w\W]+>)[^>]*|#([\w-]*))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,k=/^[\],:{}\s]*$/,E=/(?:^|:|,)(?:\s*\[)+/g,S=/\(?:["\\\/bfnrt]|u[\da-fA-F]{4}) /g,A=/"[^"\\ ]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^ -ms-/,D=/-([\da-z])/gi,L=function(e,t){return t.toUpperCase()},H=function(e){(o.addEventListener||"load"===e.type||"co mplete"===o.readyState)&&(q(),b.ready())},q=function(){o.addEventListene r?(o.removeEventListener("DOMContentLoaded",H,!1),e.removeEventListene r(" load",H,!1)):(o.detachEvent("onreadystatechange",H),e.detachEvent("o nloa d",H))};b.fn=b.prototype={jquery:p,constructor:b,init:function(e,n,r){va r i,a;if(!e)return this;if("string"==typeof e){if(i="<"===e.charAt(0)&&">"===e.charAt(e.length-1)&&e.length>=3?[null, e,null]:N.exec(e),!i||!i[1]&&n)return!n||n.jquery?(n||r).find(e):this.co nstructor(n).find(e);if(i[1]){if(n=n instanceof b?n[0]:n,b.merge(this,b.parseHTML(i[1],n&&n.nodeType?n.ownerDocument||n: o,!0)),C.test(i[1])&&b.isPlainObject(n))for(i in n)b.isFunction(this[i])?this[i](n[i]):this.attr(i,n[i]);return this}if(a=o.getElementById(i[2]),a&&a.parentNode){if(a.id!==i[2])return r.find(e);this.length=1,this[0]=a}return this.context=o,this.selector=e,this}return e.nodeType?(this.context=this[0]=e,this.length=1,this):b.isFunction(e)?r.ready(e):(e.selector!==t&&(this.selector=e.selecto
	r,this.context=e.context),b.makeArray(e,this))},selector:"",length:0,size e:function(){return this.length},toArray:function(){return h.call(this)},get:function(e){return null==e?this.toArray():0>e?this[this.length+e]:this[e]},pushStack:function(e){var t=b.merge(this.constructor(),e);return t.prevObject=this,t.context=this.context,t},each:function(e,t){return b.each(this,e,t)},ready:function(e){return b.ready.promise().done(e),this},slice:function(){return this.pushStack(h.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-1)},eq:function(e){var t=this.length,n=+e+(0>e?t:0);return this.pushStack(n>=0&&t>n?[this[n]]:[])},map:function(e){return this.pushStack(b.map(this,function(t,n){return e.call(t,n,t)}))},end:function(){return this.prevObject||this.constructor(null)},push:d,sort:[].sort,splice:[].splice},b.fn.init.prototype=b.fn,b.extend=b.fn.extend=function(){var e,n,r,i,o,a,s=arguments[0]||{},u=1,l=arguments.length,c=!1;for("boolean"==typeof s&&(c=s,s=arguments[1]||{},u=2),"object"==typeof

风险举证	s||b.isFunction(s)||(s={}),l===u&&(s=this,--u);l>u;u++)if(null!=(o=argum ents[u]))for(i in o)e=s[i],r=o[i],s!==r&&(c&&r&&(b.isPlainObject(r)||(n = b.isArray(r)))?(n?(n=!1,a=e&&b.isArray(e)?e:[]):a=e&&b.isPlainObject(e) ? e:{},s[i]=b.extend(c,a,r)):r!==t&&(s[i]=r));return s},b.extend({noConflict:function(t){return e.$===b&&(e.$=u),t&&e.jQuery===b&&(e.jQuery=s),b},isReady:!1,readyWait:1, holdReady:function(e){e?b.readyWait++:b.ready(!0)},ready:function(e){if(e===!0?!--b.readyWait:!b.isReady){if(!o.body)return setTimeout(b.ready);b.isReady=!0,e!==!0&&--b.readyWait>0||(n.resolveWith (o,[b]),b.fn.trigger&&b(o).trigger("ready").off("ready"))}},isFunction: f unction(e){return"function"===b.type(e)},isArray:Array.isArray||functi on (e){return"array"===b.type(e)},isWindow:function(e){return null!=e&&e==e.window},isNumeric:function(e){return!isNaN(parseFloat(e))& &isFinite(e)},type:function(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[m.call(e)]||"object":typeof e},isPlainObject:function(e){if(!e||"object"!==b.type(e)||e.nodeType||b. isWindow(e))return!1;try{if(e.constructor&&!y.call(e,"constructor")&&!y. call(e.constructor.prototype,"isPrototypeOf"))return!1}catch(n){return! 1 }var r;for(r in e);return r===t||y.call(e,r)},isEmptyObject:function(e) { var t;for(t in e)return!1;return!0},error:function(e){throw Error(e)},parseHTML:function(e,t,n){if(!e||"string"!=typeof e)return null;"boolean"==typeof t&&(n=t,t=!1),t=t||o;var r=C.exec(e),i=!n&&[];return r?[t.createElement(r[1])]:(r=b.buildFragment ([e],t,i),i&&b(i).remove(),b.merge([],r.childNodes))},parseJSON:functio n (n){return e.JSON&&e.JSON.parse?e.JSON.parse(n):null===n?n:"string"==typ eof n&&(n=b.trim(n),n&&k.test(n.replace(S,"@").replace(A,"]").replace (E,"")))?Function("return "+n)():(b.error("Invalid JSON: "+n),t)},parseXML:function(n){var r,i;if(!n||"string"!=typeof n)return null;try{e.DOMParser?(i=new DOMParser,r=i.parseFromString(n,"text/xml")): (r=new ActiveXObject("Microsoft.XMLDOM"),r.async="false",r.loadXML(n))} c atch(o){r=t}return r&&r.documentElement&&!r.getElementsByTagName("pars er error").length||b.error("Invalid XML: "+n),r},noop:function(){},globalEval:function(t){t&&b.trim(t)&&(e.execScr ipt||function(t){e.eval.call(e
	,t)})(t)},camelCase:function(e){return e.replace(j,"ms-").replace(D,L)},nodeName:function(e,t){return e.nodeName&&e.nodeName.toLowerCase()===t.toLowerCase()},each:function(e, t,n){var r,i=0,o=e.length,a=M(e);if(n){if(a){for(;o>i;i++)if(r=t.apply(e [i],n),r===!1)break}else for(i in e)if(r=t.apply(e[i],n),r===!1)break}el se if(a){for(;o>i;i++)if(r=t.call(e[i],i,e[i]),r===!1)break}else for(i in e)if(r=t.call(e[i],i,e[i]),r===!1)break;return e},trim:v&&!v.call("\ufeff\u00a0")?function(e){return null==e?"":v.call(e)}:function(e){return null==e?"":(e+"").replace(T,"")},makeArray:function(e,t){var n=t||[];return null!=e&&(M(Object(e))?b.merge(n,"string"==typeof e?[e]:e):d.call(n,e)),n},inArray:function(e,t,n){var r;if(t){if(g)return g.call(t,e,n);for(r=t.length,n=n?0>n?Math.max(0,r+n): n:0;r>n;n++)if(n in t&&t[n]===e)return n}return-1},merge:function(e,n){var r=n.length,i=e.length,o=0;if("number" ==typeof r)for(;r>o;o++)e[i++]=n[o];else while(n[o]!==t)e[i++]=n[o++];return e.length=i,e},grep:function(e,t,n){v ar r,i=[],o=0,a=e.length;for(n=!!n;a>o;o++)r=!!t(e[o],o),n!==r&&i.push(e [o]);return i},map:function(e,t,n){var

风险举证	r,i=0,o=e.length,a=M(e),s=[];if(a)for(;o>i;i++)r=t(e[i],i,n),null!=r&&(s[s.length]=r);else for(i in e)r=t(e[i],i,n),null!=r&&(s[s.length]=r);return f.apply([],s)},guid:1,proxy:function(e,n){var r,i,o;return"string"==typeof n&&(o=e[n],n=e,e=o),b.isFunction(e)?(r=h.call(arguments,2),i=function(){return e.apply(n||this,r.concat(h.call(arguments)))},i.guid=e.guid=e.guid||b.guid++,i):t},access:function(e,n,r,i,o, a,s){var u=0,l=e.length,c=null==r;if("object"===b.type(r)){o=!0;for(u in r)b.access(e,n,u,r[u],!0,a,s)}else if(i!==t&&(o=!0,b.isFunction(i)||(s=!0),c&&(s?(n.call(e,i),n=null):(c=n,n=function(e,t,n){return c.call(b(e),n)})),n))for(;l>u;u++)n(e[u],r,s?i:i.call(e[u],u,n(e[u],r)));return o?e:c?n.call(e):l?n(e[0],r):a},now:function(){return(new Date).getTime()}}),b.ready.promise=function(t){if(!n)if(n=b.Deferred(),"complete"===o.readyState)setTimeout(b.ready);else if(o.addEventListener)o.addEventListener("DOMContentLoaded",H,!1),e.addEventListener("load",H,!1);else{o.attachEvent("onreadystatechange",H),e.attachEvent("onload",H);var r=!1;try{r=null==e.frameElement&&o.documentElement}catch(i){}r&&r.doScroll&&function a(){if(!b.isReady){try{r.doScroll("left")}catch(e){return setTimeout(a,50)}q(),b.ready()}}()}return n.promise(t)},b.each("Boolean Number String Function Array Date RegExp Object Error".split(" "),function(e,t){l["[object "+t+"]"]=t.toLowerCase()});function M(e){var t=e.length,n=b.type(e);return b.isWindow(e)?!1:1===e.nodeType&&t?!0:"array"===n||"function"!==n&&(0===t||"number"==typeof t&&t>0&&t-1 in e)}r=b(o);var _={};function F(e){var t=_[e]={};return b.each(e.match(w)||[],function(e,n){t[n]=!0}),t}b.Callbacks=function(e){e="string"==typeof e?_[e]||F(e):b.extend({},e);var n,r,i,o,a,s,u=[],l=!e.once&&[],c=function(t){for(r=e.memory&&t,i=!0,a=s||0,s=0,o=u.length,n=!0;u&&o>a;a++)if(u[a].apply(t[0],t[1])===!1&&e.stopOnFalse){r=!1;break}n=!1,u&&(l?l.length&&c(l.shift()):r?u=[]:p.disable())},p={add:function(){if(u){var t=u.length;(function i(t){b.each(t,function(t,n){var r=b.type(n);"function"===r?e.unique&&p.has(n)||u.push(n):n&&n.length&&"string"!==r&&i(n)})})(arguments),n?o=u.length:r&&
风险举证	;&(s=t,c(r))}return this},remove:function(){return u&&b.each(arguments,function(e,t){var r;while((r=b.inArray(t,u,r))>-1)u.splice(r,1),n&&(o>=r&&o--,a>=r&&a--)}),this},has:function(e){return e?b.inArray(e,u)>-1:!(!u||!u.length)},empty:function(){return u=[],this},disable:function(){return u=l=r=t,this},disabled:function(){return!u},lock:function(){return l=t,r||p.disable(),this},locked:function(){return!l},fireWith:function(e,t){return t=t||[],t=[e,t.slice?t.slice():t],!u||i&&!l||(n?l.push(t):c(t)),this},fire:function(){return p.fireWith(this,arguments),this},fired:function(){return!!i}};return p},b.extend({Deferred:function(e){var t=[["resolve","done",b.Callbacks("once memory"),"resolved"],["reject","fail",b.Callbacks("once memory"),"rejected"],["notif

6	cookie 没有设置httponly标志位【原理扫描】
风险等级	低
深信服漏洞编号	SF-2021-00870
CVE编号	-

CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	HttpOnly 主要是为了限制web页面程序的browser端script程序读取cookie，防止恶意代码获取客户的敏感信息。
风险影响	远程攻击者可以利用此漏洞获取敏感信息
解决方案	为SetCookie配置HttpOnly属性
风险举证	举证描述： - 页面：http://th-storage.com 请求： GET HTTP/1.1 Host: th-storage.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 404 Not Found Cache-Control: private Content-Length: 2320 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDACCDDDDD=BKEMNJMCHNNILFNAFLMAODLC; path=/ Date: Wed, 19 Feb 2025 10:00:24 GMT Connection: keep-alive <!DOCTYPE html PUBLIC " -//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 网站访问报错</title> <style type="text/css"> * { padding:0; margin:0;} li { list-style:none;} img { border:none;} .clear { zoom:1;} .clear:after { content:'\20'; clear:both; display:block;}

7	OPTIONS方法启用【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00126
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此Web服务器上启用了HTTP OPTIONS方法。 OPTIONS方法提供了Web服务器支持的方法列表，它表示对有关由Request-URI标识的请求/响应链上可用的通信选项的信息的请求。
风险影响	OPTIONS方法可能会公开敏感信息，这些信息可能有助于恶意用户准备更高级的攻击。
解决方案	建议在Web服务器上禁用OPTIONS方法。
风险举证	举证描述： - 页面：http://th-storage.com 请求： OPTIONS HTTP/1.1 Host: th-storage.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive Content-Length: 0 响应： HTTP/1.1 200 OK Allow: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/7.5 Public: OPTIONS, TRACE, GET, HEAD, POST Date: Wed, 19 Feb 2025 10:00:25 GMT Connection: keep-alive Content-Length: 0

8	ASP.NET版本泄露【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00137
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此Web应用程序返回的HTTP响应包括名为 X-AspNet-Version 的标头。 Visual Studio使用此标头的值来确定正在使用哪个版本的ASP.NET。 对于生产站点而言，这不是必需的，应该禁用。
风险影响	HTTP标头可能会泄露敏感信息。 此信息可用于发起进一步的攻击。
解决方案	对web.config文件应用以下更改以防止ASP.NET版本泄漏：<System.Web> <httpRuntime enable VersionHeader="false" /> </System.Web>
风险举证	举证描述： - 页面：http://th-storage.com 请求： GET /|~.aspx HTTP/1.1 Host: th-storage.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 500 Internal Server Error Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/7.5 X-AspNet-Version: 2.0.50727 Date: Wed, 19 Feb 2025 10:00:19 GMT Connection: keep-alive Content-Length: 2907 <html> <head> <title>运行时错误</title> <style> body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;} p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px} b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px} H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red } H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon } pre {font-family:"Lucida Console";font-size: .9em} .marker {font-weight: bold; color: black;text-decoration: none;} .version {color: gray;} .error {margin-bottom: 10px;} .expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:hand; } </style> </head>

9	Microsoft IIS版本泄露【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00136
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此web应用程序返回的HTTP响应包括名为Server的头。此头的值包括Microsoft IIS服务器的版本。
风险影响	HTTP头可能会泄漏敏感信息。这些信息可以进行发动进一步的攻击。

解决方案	Microsoft IIS应该配置为从响应中删除不需要的HTTP响应标头。 有关更多信息，请参考网络参考。
风险举证	举证描述： - 页面：http://th-storage.com 请求： GET HTTP/1.1 Host: th-storage.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 404 Not Found Cache-Control: private Content-Length: 2320 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDACCDDDDD=DIEMNJMCCCGIMHHJJOKEBLDC; path=/ Date: Wed, 19 Feb 2025 10:00:23 GMT Connection: keep-alive <!DOCTYPE html PUBLIC " -//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 网站访问报错</title> <style type="text/css"> * { padding:0; margin:0;} li { list-style:none;} img { border:none;} .clear { zoom:1;} .clear:after { content:'\20'; clear:both; display:block;}

10	general 未设置cookie的Secure标志位【原理扫描】
风险等级	低
深信服漏洞编号	SF-2016-00025
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	通用型(general)漏洞并不针对某一系统，其在各类系统中都有可能存在。Cookie Without Secure Flag Set是指服务器Set-Cookie消息头中未设置可选属性Secure，如果服务器设置这个属性，那么cookie只能在HTTPS请求中提交。
风险影响	影响所有Set-Cookie消息头中未设置可选属性Secure的系统
解决方案	为cookie设置Secure属性
风险举证	举证描述： - 页面：http://th-storage.com 请求： GET HTTP/1.1 Host: th-storage.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 404 Not Found Cache-Control: private Content-Length: 2320 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDACCDDDDD=BKEMNJMCHNNILFNAFLMAODLC; path=/ Date: Wed, 19 Feb 2025 10:00:24 GMT Connection: keep-alive <!DOCTYPE html PUBLIC " -//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 网站访问报错</title> <style type="text/css"> * { padding:0; margin:0;} li { list-style:none;} img { border:none;} .clear { zoom:1;} .clear:after { content:'\20'; clear:both; display:block;}

5.1.3 弱口令

该资产不存在弱口令风险。

5.1.3 登录入口

该资产不存在登录入口风险。

5.2 http://www.th-storage.com

5.2.1 系统漏洞

1	IIS FTPSVC远程拒绝服务漏洞(CVE-2010-3972)
风险等级	高
深信服漏洞编号	SF-0005-17606
CVE编号	CVE-2010-3972
CNNVD编号	CNNVD-201012-307
CNVD编号	
Bugtraq编号	45542
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。Windows 7 IIS 7.5处理请求中的Telnet协议转义时存在的堆溢出问题，远程可以利用此漏洞导致服务器程序崩溃，拒绝服务合法用户或导致执行任意代码。
风险影响	影响IIS:7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS11-004）以及相应补丁 MS11-004：Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-004
风险举证	IIS:7.5

2	IIS FastCGI请求头远程溢出漏洞(CVE-2010-2730)
风险等级	高
深信服漏洞编号	SF-0005-17607
CVE编号	CVE-2010-2730
CNNVD编号	CNNVD-201009-133
CNVD编号	CNVD-2010-2000

Bugtraq编号	43138
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。对于启用了FastCGI功能的IIS服务器，远程攻击者可以通过提交特制的HTTP请求触发缓冲区溢出，导致执行任意代码。
风险影响	影响IIS:7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS10-065）以及相应补丁 MS10-065：Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-065
风险举证	IIS:7.5

3	IIS 重复参数请求拒绝服务漏洞(CVE-2010-1899)
风险等级	中
深信服漏洞编号	SF-0005-17608
CVE编号	CVE-2010-1899
CNNVD编号	CNNVD-201009-126
CNVD编号	CNVD-2010-1985
Bugtraq编号	43140
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。IIS中的脚本处理代码在处理重复的参数请求时存在栈溢出漏洞，远程攻击者可以通过对IIS所承载网站的ASP页面发送特制URI请求来利用这个漏洞，导致服务崩溃。
风险影响	影响IIS:6.0版本,7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS10-065）以及相应补丁 MS10-065：Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-065
风险举证	IIS:7.5

5.2.2 web漏洞

1	SQL注入攻击【原理扫描】
风险等级	高
深信服漏洞编号	SF-0000-0378
CVE编号	-
CNNVD编号	

CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	该网站可能易受SQL注入攻击。 SQL注入漏洞允许攻击者通过操纵用户输入改变后端SQL语句。若Web应用程序收到用户输入时直接放入SQL语句，而没有正确过滤危险字符时，会发生SQL注入。
风险影响	攻击者可以在受害网站上执行任意SQL语句。可能会破坏数据库的完整性或暴露敏感信息。甚至执行shell命令，威胁整个网站服务器。
解决方案	严格过滤用户输入的数据。
风险举证	举证描述： URL encoded GET input id was set to 399/(3*2-5) Tests performed: ,,,,, Original value: 399 页面： http://www.th-storage.com/news_detail.asp?id=399 请求： GET /news_detail.asp?id=399/(3*2-5) HTTP/1.1 X-Requested-With: XMLHttpRequest Referer: http://www.th-storage.com/news_detail.asp?id=399 Connection: Keep-Alive Cookie: ASPSESSIONIDAABABCCC=NBOLIHMCHPALEPLKMGKLBFIE; path=/ User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 响应： HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html Content-Encoding: gzip Vary: Accept-Encoding Server: Microsoft-IIS/7.5 Date: Wed, 19 Feb 2025 11:44:26 GMT Content-Length: 11308 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title>□□ □□□□□□□□□□□□□□□□□□□□□¨□□□□□□□□□□ □□□□□□□□° □□□□□□□□□□é□□_□□□□□□□□□□□□□□□ □□□□è□□□□□□□□□é□□□ □□□□</title> <meta name="keywords" content="□□□□□□□ □□□□,□□□□□□□□□□□□□□ □□□□è□□□□□□□□□é□□□ □□□□□"> <meta name="description" content="□□□□□□□□□□□□□□□ □□□□è□□□□□□□□□é□□□ □□□□□□□□□□□□□□□□□è□□□□□□□□□é□□□ □□□□□□ ¨è□□□□□□ □□□□□□□□□□¨□□□□è□□□□□4000□□□□□□□□ □□□□□□□□□□□□□□□□□ □□□□□□¨□□□□ ¨□□□□□□□□¨□□□□é□□□□° □□□□□□□□□□□□□□□□□□□ □□□□□ □□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□ □□□□è□□□□□□□□□□□□□□□□□□□§□□□¨□□□□□¨é□□ □□□□□□□□□□□□□□□□é□ □□□□□□□□ □□□□□□□□□ ¨□□□□□¨□□□□□□□□¤□□□□□□□□□□□□□□□□□□□□□□□□□□ □"> <link href="css/css.css" rel="stylesheet" type="text/css" /> <link href="css/style.css" rel="stylesheet" type="text/css" /> <link href="css/pro.css" rel="stylesheet" type="text/css" /> <link rel="stylesheet" href="wei/reset.css" type="text/css" media="screen" charset="utf-8"> <script src="wei/jQuery.js" type="text/javascript" charset="utf-8"></script> <script src="wei/new.js" type="text/javascript" charset="utf-8"></script> </head> <body> <script> var _hmt = _hmt || []; (function() { var hm = document.createElement("script"); hm.src = "https://hm.baidu.com/hm.js?597805b8f3a912caaa0e90184d25abc0"; var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(hm, s); })(); </script> <div

	class="w1180"> <div class="c1"> <div class="d1">□□□è□□□□¨è□□é□□□□□□□□□□□□□□□□ □□□□è□□□□□□□□□□é□□□ □□□□□□□□□□□□□□□□° □□□□è □□□□□□□□¨□□□□□□□□□□</div> <div class="d2"> <div class="n-htop por z2"> <div class="m fr por curp"> □□□□□□□ <img src="wei/mallewm.jpg" width="108" alt="" class="poa dn"> </div> <p style="text-align:right; padding-right:80px;">□□□è□□è□□□□□□□□□010-62780307 / 82863225</p> </div> </div> <div class="d3"> <table cellspacing="0" cellpadding="0" width="220" align="right" border="0"> <tbody> </tbody> <form action="products.asp" method="post" name="search" id="search"> <tr> <td width="75%" align="left" valign="middle" background="images/index_04.jpg"><input id="k" name="k" size="17" maxlength="5
风险举证	0" style="BORDER: #cccccc 0px solid;HEIGHT: 16px; BACKGROUND-COLOR: #9e9e9e; color:#FFFFFF" onfocus="if(this.value=='Search') this.value=''" onblur="if(this.value=='') this.value='Search'" value="Search"/></td> <td width="25%" align="left" valign="middle" ><input type="image" height="55" width="49" src="images/index_05.jpg" align="absmiddle" name="submit" /></td> </tr> </form> </table> </div> </div> <div class="headerr "> <div class="wrap"> <div class="js-logo"></div> <h3>é□□é□□</h3> <h3 class="see">□□§□□□□□□□□□□□</h3> □ □□□□ □□□□□□□□□§ □□ □□□□□□□□□□DVD□□□□□□□□□§□ □□□□□ 4.7G □□ □□□□□□□□□□BDè□□□ □□□□□□□□□□§□ □□□□□□□□25G□□□ □□ □□□□□□□□□□BDè□□□ □□□□□□□□□□§□ □□□□□□□□50G□□□ □□ □□□□□□□□□□BDè□□□ □□□□□□□□□□§□ □□□□128G□□□25□□□è□ □□□ □□□□□□□□□§

	□□ □□□□□□□□□□□□□□□□□□§□ □□□□ □□ □□□□□□□□□é□□□ □□□□□□□□□° DVD□□□□□□□□§□ □□□□4.7G □□ □□□□□□□□□□□□□□□□□□§BD25G□ □□□□ □□ □□□□□□□□□é□□□ □□□□□□□□□° □□□□□□□□§BD25G□ □□□□ □□□è□□□□§ □□ □□□□□□□□□CD □□ □□□□□□□□□DVD□ □□□□ A+□□§ □ □ □□□□□□□□□DVD□ □□□□ □□ □□□□□□□□□□□□□□□□□□° DVD□ □□□□ <a href="products_
风险举证	detail.asp?id=1052">□□ □□□□□□□□□é□□□¤□DVD□ □□□□ □□ □□□□□□□□□□□□□□□□□DVD□ □□□□ □□ □□□□□□□□□□□° □□□ DVD□ □□□□ □□ □□□□□□□□□□□□ □§□□ □□□□ □ □□□□□□□□□□□□□□□ □□□□□□□□§□ □□□□□□□□□□□□□□□ □□□□□□□□§□ □□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□ □¤□□□□è□ è□□DVD/CD□□□□□□□□□□□ □ ¨è□□□□¨□□□□□□° □□□□□□□□□□□□□□□□□□□ □ □é□¨□□§ □□□□□□□□§DVD□ □□□□□□□□□° □□□□□□□□□□□□□□□□□□□ □□□□□□□□§BD□ □□□□□□□□□° □□□□□□□□□□□□□□□□□□□ □□□□□□□□§DVD□ □□□□□□□□□° □□□□□□□□□□□□□□□□□□□ □□□□□□□□§BD□ □□□□□□□□□° □□□□□□□□□□□□□□□□□□□ è□□é□□□□§ □□□□□□□□§DVD□ □□□□□□□□□° □□□□□□□□□□□□□□□□□□-100□□□ □□□□□□□□§BD□ □□□□□□□□□° □□□□□□□□□□□□□□□□□□-100□□□

	□□□□□□□§DVD□□□□□□□□□□° □□□□□□□□□□□□□□□□-100□□□ □□□□□□□§BD□□□□□□□□□□° □□□□
风险举证	□□□□□□□□□□□-100□□□ é□□□□□□□§ □□□□□□□□§DVD□□□□□□□□□□° □□□□□□□□□□□□□□□□-150□□□ □□□□□□□§BD□□□□□□□□□□° □□□□□□□□□□□□□□□□-150□□□ <a href="products_detail.asp?id=1082">□□□□□□□§DVD□□□□□□□□□□° □□□□□□□□□□

2	Javascript库不安全【原理扫描】
风险等级	中
深信服漏洞编号	SF-0000-0382
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	正在使用易受攻击的Javascript库。 已报告此版本的Javascript库存在一个或多个漏洞。 有关受影响的库和所报告的漏洞的更多信息，请查阅攻击详细信息和Web参考。
风险影响	有关更多信息，请参考Web参考。
解决方案	升级到最新版本。
	举证描述： Detected Javascript library jquery version 1.9.1. The version was detected from contents, and contents. 页面： http://www.th-storage.com/wei/jQuery.js 请求： GET /wei/jQuery.js HTTP/1.1 Accept : */* Cookie : ASPSESSIONIDAABABCCC=OBOLIHMCLNAGBIJEIBFNBJMD Referer : http://www.th-storage.com/ User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36 响应： HTTP/1.1 200 OK Content-Type :

风险举证	application/x-javascript Content-Encoding : gzip Last-Modified : Wed, 20 Sep 2017 06:04:10 GMT Accept-Ranges : bytes ETag : "0a98846d631d31:0" Vary : Accept-Encoding Server : Microsoft-IIS/7.5 Date : Wed, 19 Feb 2025 11:27:26 GMT Content-Length : 32837/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license */(function(e,t){var n,r,i=typeof t,o=e.document,a=e.location,s=e.jQuery, u=e.$,l={},c=[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,g=c.indexOf,m=l. toString,y=l.hasOwnProperty,v=p.trim,b=function(e,t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,w=/\S+/ g,T=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:(<[\w\W]+>)[^>]*|#([\w-] *))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,k=/^[\],:{}\s]*$/,E=/(?:^|:|,)(?:\s *\[)+/g,S=/\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,A=/"[^"\\ ]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^-ms-/,D=/-([\da-z])/gi,L=function(e,t){return t.toUpperCase()},H=function(e){(o.addEv e ntListener||"load"===e.type||"complete"===o.readyState)&&(q(),b.ready())},q=function(){o.addEventListener?(o.removeEventListener("DOMContentLo ad ed",H,!1),e.removeEventListener("load",H,!1)):(o.detachEvent("onready sta techange",H),e.detachEvent("onload",H))};b.fn=b.prototype={jquery:p, cons tructor:b,init:function(e,n,r){var i,a;if(!e)return this;if("string"==typeof e){if(i="<"===e.charAt(0)&&">"===e.charAt(e.len gth-1)&&e.length>=3?[null,e,null]:N.exec(e),!i||!i[1]&&n)return!n||n.jq u ery?(n||r).find(e):this.constructor(n).find(e);if(i[1]){if(n=n instanceof b?n[0]:n,b.merge(this,b.parseHTML(i[1],n&&n.nodeType?n.ownerD ocument||n:o,!0)),C.test(i[1])&&b.isPlainObject(n))for(i in n)b.isFunction(this[i])?this[i](n[i]):this.attr(i,n[i]);return this}if(a=o.getElementById(i[2]),a&&a.parentNode){if(a.id!==i[2])return r.find(e);this.length=1,this[0]=a}return this.context=o,this.selector=e,this}return e.nodeType?(this.context=this[0]=e,this.length=1,this):b.isFunction(e)?r. ready(e):(e.selector!==t&&(this.selector=e.selector,this.context=e.cont e xt),b.makeArray(e,this))},selector:"",length:0,size:function(){return this.length},toArray:function(){return h.call(this)},get:function(e){return null==e?this.toArray():0>e?this[thi s.length+e]:this[e]},pushStack:function(e){var t=b.merge(this.constructor(),e);return t.prevObject=this,t.context=this.context,t},each:function(e,t){return b.each(this,e,t)},ready:function(e){return b.ready.promise().done(e),this},slice:function(){return this.pushStack(h.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-1)},eq:function(e){var t=this.length,n=+e+(0>e?t:0);return this.pushStack(n>=0&&t>n?[this[n]]:[])},map:function(e){return this.pushStack(b.map(this,function(t,n){retur n e.call(t,n,t)}))},end:function(){return this.prevObject||this.constructor(null)},push:d,sort:[].sort,splice:[].s plice},b.fn.init.prototype=b.fn,b.extend=b.fn.extend=
	function(){var e,n,r,i,o,a,s=arguments[0]||{},u=1,l=arguments.length,c=! 1;for("boolean"==typeof s&&(c=s,s=arguments[1]||{},u=2),"object"==typeof s||b.isFunction(s)||(s={}),l===u&&(s=this,--u);l>u;u++)if(null!=(o=argu ments[u]))for(i in o)e=s[i],r=o[i],s!==r&&(c&&r&&(b.isPlainObject(r)||(n =b.isArray(r)))?(n?(n=!1,a=e&&b.isArray(e)?e:[]):a=e&&b.isPlainObject(e)? e:{},s[i]=b.extend(c,a,r)):r!==t&&(s[i]=r));return s},b.extend({noConflict:function(t){return e.$===b&&(e.$=u),t&&e.jQuery===b&&(e.jQuery=s),b},isReady:!1,readyWait:1,

风险举证	holdReady:function(e){e?b.readyWait++:b.ready(!0)},ready:function(e){if(e===!0?!--b.readyWait:!b.isReady){if(!o.body)return setTimeout(b.ready);b.isReady=!0,e!==!0&&--b.readyWait>0||(n.resolveWith(o,[b]),b.fn.trigger&&b(o).trigger("ready").off("ready"))}},isFunction:f unction(e){return"function"===b.type(e)},isArray:Array.isArray||function (e){return"array"===b.type(e)},isWindow:function(e){return null!=e&&e==e.window},isNumeric:function(e){return!isNaN(parseFloat(e))&&isFinite(e)},type:function(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[m.call(e)]||"object":typeof e},isPlainObject:function(e){if(!e||"object"!==b.type(e)||e.nodeType||b.isWindow(e))return!1;try{if(e.constructor&&!y.call(e,"constructor")&&!y.call(e.constructor.prototype,"isPrototypeOf"))return!1}catch(n){return!1 }var r;for(r in e);return r===t||y.call(e,r)},isEmptyObject:function(e){ var t;for(t in e)return!1;return!0},error:function(e){throw Error(e)},parseHTML:function(e,t,n){if(!e||"string"!=typeof e)return null;"boolean"==typeof t&&(n=t,t=!1),t=t||o;var r=C.exec(e),i=!n&&[];return r?[t.createElement(r[1])]:(r=b.buildFragment([e],t,i),i&&b(i).remove(),b.merge([],r.childNodes))},parseJSON:functio n (n){return e.JSON&&e.JSON.parse?e.JSON.parse(n):null===n?n:"string"==typ eof n&&(n=b.trim(n),n&&k.test(n.replace(S,"@").replace(A,"]").replace(E," ")))?Function("return "+n)():(b.error("Invalid JSON: "+n),t)},parseXML:function(n){var r,i;if(!n||"string"!=typeof n)return null;try{e.DOMParser?(i=new DOMParser,r=i.parseFromString(n,"text/xml")):(r=new ActiveXObject("Microsoft.XMLDOM"),r.async="false",r.loadXML(n))}c atch(o){r=t}return r&&r.documentElement&&!r.getElementsByTagName("pars er error").length||b.error("Invalid XML: "+n),r},noop:function(){},globalEval:function(t){t&&b.trim(t)&&(e.execScript||function(t){e.eval.call(e,t)})(t)},camelCase:function(e){return e.replace(j,"ms-").replace(D,L)},nodeName:function(e,t){return e.nodeName&&e.nodeName.toLowerCase()===t.toLowerCase()},each:function(e,t,n){var r,i=0,o=e.length,a=M(e);if(n){if(a){for(;o>i;i++)if(r=t.apply(e[i],n),r===!1)break}else for(i in e)if(r=t.apply(e[i],n),r===!1)break}el se if(a){for(;o>i;i++)if(r=t.call(e[i],i,e[i]),r===!1)break}else for(i in e)if(r=t.call(e[i],i,e[i]),r===!1)break;return e},trim:v&&!v.call("\ufeff\u00a0")?function(e){return null==e?"":v.call(e)}:function(e){return null==e?"":(e+"").replace(T,"")},makeArray:function(e,t){var n=t||[];return null!=e&&(M(Object(e))?b.merge(n,"string"==typeof e?[e]:e):d.call(n,e)),n},inArray:function(e,t,n){var r;if(t){if(g)return g.call(t,e,n);for(r=t.length,n=n?0>n?Math.max(0,r+n):n:0;r>n;n++)if(n in t&&t[n]===e)return n}return-1},merge:function(e,n){var r=n.length,i=e.l
	ength,o=0;if("number"==typeof r)for(;r>o;o++)e[i++]=n[o];else while(n[o]!==t)e[i++]=n[o++];return e.length=i,e},grep:function(e,t,n){var r,i=[],o=0,a=e.length;for(n=!!n;a>o;o++)r=!!t(e[o],o),n!==r&&i.push(e[o]);return i},map:function(e,t,n){var r,i=0,o=e.length,a=M(e),s=[];if(a)for(;o>i;i++)r=t(e[i],i,n),null!=r&&(s[s.length]=r);else for(i in e)r=t(e[i],i,n),null!=r&&(s[s.length]=r);return f.apply([],s)},guid:1,proxy:function(e,n){var r,i,o;return"string"==typeof n&&(o=e[n],n=e,e=o),b.isFunction(e)?(r=h.call(arguments,2),i=function(){return e.apply(n||this,r.concat(h.call(arguments)))},i.guid=e.guid=e.guid||b.guid++,i):t},access:function(e,n,r,i,o,a,s){var u=0,l=e.length,c=null==r;if("object"===b.type(r)){o=!0;for(u

风险举证	in r)b.access(e,n,u,r[u],!0,a,s)}else
	if(i!==t&&(o=!0,b.isFunction(i)||(s=!0),c&&(s?(n.call(e,i),n=null):(c=n,
	n=function(e,t,n){return c.call(b(e),n)})),n))for(;l>u;u++)n(e[u],r,s?i:
	i.call(e[u],u,n(e[u],r)));return o?e:c?n.call(e):l?n(e[0],r):a},now:fun
	c tion(){return(new Date).getTime()}}),b.ready.promise=function(t){if(!n)
	i f(n=b.Deferred(),"complete"===o.readyState)setTimeout(b.ready);else
	if(o.addEventListener)o.addEventListener("DOMContentLoaded",H,!1),e.addE
	ventListener("load",H,!1);else{o.attachEvent("onreadystatechange",H),e.
	a ttachEvent("onload",H);var r=!1;try{r=null==e.frameElement&&o.document
	El ement}catch(i){}r&&r.doScroll&&function
	a(){if(!b.isReady){try{r.doScroll("left")}catch(e){return
	setTimeout(a,50)}q(),b.ready()}}()}return n.promise(t)},b.each("Boolean
	Number String Function Array Date RegExp Object Error".split(" ")
	,function(e,t){l["[object "+t+"]"]=t.toLowerCase()});function M(e){var
	t=e.length,n=b.type(e);return b.isWindow(e)?!1:1===e.nodeType&&t?!0:"arr
	ay"===n||"function"!==n&&(0===t||"number"==typeof t&&t>0&&t-1 in
	e)}r=b(o);var _={};function F(e){var t=_[e]={};return
	b.each(e.match(w)||[],function(e,n){t[n]=!0}),t}b.Callbacks=function(e){
	e="string"==typeof e?_[e]||F(e):b.extend({},e);var
	n,r,i,o,a,s,u=[],l=!e.once&&[],c=function(t){for(r=e.memory&&t,i=!0,a=s||
	0,s=0,o=u.length,n=!0;u&&o>a;a++)if(u[a].apply(t[0],t[1])===!1&&e.stop
	O nFalse){r=!1;break}n=!1,u&&(l?l.length&&c(l.shift()):r?u=[]:p.disable()
	) },p={add:function(){if(u){var t=u.length;(function
	i(t){b.each(t,function(t,n){var r=b.type(n);"function"===r?e.unique&&p.h
	as(n)||u.push(n):n&&n.length&&"string"!==r&&i(n)})})(arguments),n?o=u.l
	e ngth:r&&(s=t,c(r))}return this},remove:function(){return
	u&&b.each(arguments,function(e,t){var
	r;while((r=b.inArray(t,u,r))>-1)u.splice(r,1),n&&(o>=r&&o--,a>=r&&a--)}),
	this},has:function(e){return e?b.inArray(e,u)>-1:!(!u||!u.length)},empt
	y: function(){return u=[],this},disable:function(){return
	u=l=r=t,this},disabled:function(){return!u},lock:function(){return
	l=t,r||p.disable(),this},locked:function(){return!l},fireWith:function(e,
	t){return t=t||[],t=[e,t.slice?t.slice():t],!u||i&&!l||(n?l.push(t):c(t)
	) ,this},fire:function(){return p.fireWith(this,arguments),this},fired:f
	un ction(){return!!i}};return p},b.extend({Deferred:function(e){var
	t=[["resolve","done",b.Callbacks("once
	memory"),"resolved"],["reject","fail",b.Callbacks("once
	memory"),"rejected"],["notif

3	Javascript库不安全【原理扫描】
风险等级	中
深信服漏洞编号	SF-0000-0382
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	正在使用易受攻击的Javascript库。 已报告此版本的Javascript库存在一个或多个漏洞。 有关受影响的库和所报告的漏洞的更多信息，请查阅攻击详细信息和Web

	参考。
风险影响	有关更多信息，请参考Web参考。
解决方案	升级到最新版本。
风险举证	举证描述： Detected Javascript library jquery version 1.9.1. The version was detected from contents, and contents. 页面： http://www.th-storage.com/wei/jquery.js 请求： GET /wei/jquery.js HTTP/1.1 Cookie : ASPSESSIONIDAABABCCC=NBOLIHMCHPALEPLKMGKLBFIE; path=/ User-Agent : Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 响应： HTTP/1.1 200 OK Content-Type : application/x-javascript Content-Encoding : gzip Last-Modified : Wed, 20 Sep 2017 06:04:10 GMT Accept-Ranges : bytes ETag : "0a98846d631d31:0" Vary : Accept-Encoding Server : Microsoft-IIS/7.5 Date : Wed, 19 Feb 2025 11:29:03 GMT Content-Length : 32837/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license */(function(e,t){var n,r,i=typeof t,o=e.document,a=e.location,s=e.jQuery,u=e.$,l={},c=[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,g=c.indexOf,m=l.toString,y=l.hasOwnProperty,v=p.trim,b=function(e,t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,w=/\S+/g,T=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:(<[\w\W]+>)[^>]*|#([\w-]*))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,k=/^[\],:{}\s]*$/,E=/(?:^|:|,)(?:\s*\[)+/g,S=/\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,A=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^-ms-/,D=/-([\da-z])/gi,L=function(e,t){return t.toUpperCase()},H=function(e){(o.addEventListener||"load"===e.type||"complete"===o.readyState)&&(q(),b.ready())},q=function(){o.addEventListener?(o.removeEventListener("DOMContentLoaded",H,!1),e.removeEventListener("load",H,!1)):(o.detachEvent("onreadystatechange",H),e.detachEvent("onload",H))};b.fn=b.prototype={jquery:p,constructor:b,init:function(e,n,r){var i,a;if(!e)return this;if("string"==typeof e){if(i="<"===e.charAt(0)&&">"===e.charAt(e.length-1)&&e.length>=3?[null,e,null]:N.exec(e),!i||!i[1]&&n)return!n||n.jquery?(n||r).find(e):this.constructor(n).find(e);if(i[1]){if(n=n instanceof b?n[0]:n,b.merge(this,b.parseHTML(i[1],n&&n.nodeType?n.ownerDocument||n:o,!0)),C.test(i[1])&&b.isPlainObject(n))for(i in n)b.isFunction(this[i])?this[i](n[i]):this.attr(i,n[i]);return this}if(a=o.getElementById(i[2]),a&&a.parentNode){if(a.id!==i[2])return r.find(e);this.length=1,this[0]=a}return this.context=o,this.selector=e,this}return e.nodeType?(this.context=this[0]=e,this.length=1,this):b.isFunction(e)?r.ready(e):(e.selector!==t&&(this.selector=e.selector,this.context=e.context),b.makeArray(e,this))},selector:"",length:0,size:function(){return this.length},toArray:function(){return h.call(this)},get:function(e){return null==e?this.toArray():0>e?this[this.length+e]:this[e]},pushStack:function(e){var t=b.merge(this.constructor(),e);return t.prevObject=this,t.context=this.context,t},each:function(e,t){return b.each(this,e,t)},ready:function(e){return b.ready.promise().done(e),this},slice:function(){return this.pushStack(h.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-1)},eq:function(e){var t=this.length,n=+e+(0>e?t:0);return this.pushStack(n>=0&&t>n?[this[n]]:[])},map:function(e){return this.pushStack(b.map(this,function(t,n){return

	e.call(t,n,t)}))},end:function(){return this.prevObject||this.constructor(null)},push:d,sort:[].sort,splice:[].splice},b.fn.init.prototype=b.fn,b.extend=b.fn.extend=function(){var e,n,r,i,o,a,s=arguments[0]||{},u
风险举证	=1,l=arguments.length,c=!1;for("boolean"==typeof s&&(c=s,s=arguments[1]||{},u=2),"object"==typeof s||b.isFunction(s)||(s={}),l===u&&(s=this,--u);l>u;u++)if(null!=(o=arguments[u]))for(i in o)e=s[i],r=o[i],s!==r&&(c&&r&&(b.isPlainObject(r)||(n=b.isArray(r)))?(n?(n=!1,a=e&&b.isArray(e)?e:[]):a=e&&b.isPlainObject(e)?e:{},s[i]=b.extend(c,a,r)):r!==t&&(s[i]=r));return s},b.extend({noConflict:function(t){return e.$===b&&(e.$=u),t&&e.jQuery===b&&(e.jQuery=s),b},isReady:!1,readyWait:1,holdReady:function(e){e?b.readyWait++:b.ready(!0)},ready:function(e){if(e===!0?!--b.readyWait:!b.isReady){if(!o.body)return setTimeout(b.ready);b.isReady=!0,e!==!0&&--b.readyWait>0||(n.resolveWith(o,[b]),b.fn.trigger&&b(o).trigger("ready").off("ready"))}},isFunction:function(e){return"function"===b.type(e)},isArray:Array.isArray||function(e){return"array"===b.type(e)},isWindow:function(e){return null!=e&&e==e.window},isNumeric:function(e){return!isNaN(parseFloat(e))&&isFinite(e)},type:function(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[m.call(e)]||"object":typeof e},isPlainObject:function(e){if(!e||"object"!==b.type(e)||e.nodeType||b.isWindow(e))return!1;try{if(e.constructor&&!y.call(e,"constructor")&&!y.call(e.constructor.prototype,"isPrototypeOf"))return!1}catch(n){return!1}var r;for(r in e);return r===t||y.call(e,r)},isEmptyObject:function(e){var t;for(t in e)return!1;return!0},error:function(e){throw Error(e)},parseHTML:function(e,t,n){if(!e||"string"!=typeof e)return null;"boolean"==typeof t&&(n=t,t=!1),t=t||o;var r=C.exec(e),i=!n&&[];return r?[t.createElement(r[1])]:(r=b.buildFragment([e],t,i),i&&b(i).remove(),b.merge([],r.childNodes))},parseJSON:function

	(n){return e.JSON&&e.JSON.parse?e.JSON.parse(n):null===n?n:"string"==typ eof n&&(n=b.trim(n),n&&k.test(n.replace(S,"@").replace(A,"]").replace(E," ")))?Function("return "+n)():(b.error("Invalid JSON: " +n),t)},parseXML:function(n){var r,i;if(!n||"string"!=typeof n)return null;try{e.DOMParser?(i=new DOMParser,r=i.parseFromString(n,"text/xml")): (r=new ActiveXObject("Microsoft.XMLDOM"),r.async="false",r.loadXML(n))} c atch(o){r=t}return r&&r.documentElement&&!r.getElementsByTagName("pars er error").length||b.error("Invalid XML: " +n),r},noop:function(){},globalEval:function(t){t&&b.trim(t)&&(e.execScr ipt||function(t){e.eval.call(e,t)})(t)},camelCase:function(e){return e.replace(j,"ms-").replace(D,L)},nodeName:function(e,t){return e.nodeName&&e.nodeName.toLowerCase()===t.toLowerCase()},each:function(e, t,n){var r,i=0,o=e.length,a=M(e);if(n){if(a){for(;o>i;i++)if(r=t.apply(e [i],n),r===!1)break}else for(i in e)if(r=t.apply(e[i],n),r===!1)break} el se if(a){for(;o>i;i++)if(r=t.call(e[i],i,e[i]),r===!1)break}else for(i in e)if(r=t.call(e[i],i,e[i]),r===!1)break;return e},trim:v&&!v.call("\ufeff\u00a0")?function(e){return null==e?"":v.call(e)}:function(e){return null==e?"":(e+"").replace(T,"")},makeArray:function(e,t){var n=t||[];return null!=e&&(M(Object(e))?b.merge(n,"string"==typeof e?[e]:e):d.call(n,e)),n},inArray:function(e,t,n){var r;if(t){if(g)return g.call(t,e,n);for(r=t.length,n=n?0>n?Math.max(0,r+n): n:0;r>n;n++)if(n in t&&t[n]===e)return n}return-1},merge:function(e,n){var r=n.length,i=e.length,o=0;if("number" ==typeof r)for(;r>o;o++
风险举证	)e[i++]=n[o];else while(n[o]!==t)e[i++]=n[o++];return e.length=i,e},grep:function(e,t,n){var r,i=[],o=0,a=e.length;for(n=!!n;a>o;o++)r=!!t(e[o],o),n!==r&&i.push(e[o]);return i},map:function(e,t,n){var r,i=0,o=e.length,a=M(e),s=[];if(a)for(;o>i;i++)r=t(e[i],i,n),null!=r&&(s[s.length]=r);else for(i in e)r=t(e[i],i,n),null!=r&&(s[s.length]=r);return f.apply([],s)},guid:1,proxy:function(e,n){var r,i,o;return"string"==typeof n&&(o=e[n],n=e,e=o),b.isFunction(e)?(r=h.call(arguments,2),i=function(){return e.apply(n||this,r.concat(h.call(arguments)))},i.guid=e.guid=e.guid||b.guid++,i):t},access:function(e,n,r,i,o,a,s){var u=0,l=e.length,c=null==r;if("object"===b.type(r)){o=!0;for(u in r)b.access(e,n,u,r[u],!0,a,s)}else if(i!==t&&(o=!0,b.isFunction(i)||(s=!0),c&&(s?(n.call(e,i),n=null):(c=n,n=function(e,t,n){return c.call(b(e),n)})),n))for(;l>u;u++)n(e[u],r,s?i:i.call(e[u],u,n(e[u],r)));return o?e:c?n.call(e):l?n(e[0],r):a},now:function(){return(new Date).getTime()}}),b.ready.promise=function(t){if(!n)if(n=b.Deferred(),"complete"===o.readyState)setTimeout(b.ready);else if(o.addEventListener)o.addEventListener("DOMContentLoaded",H,!1),e.addEventListener("load",H,!1);else{o.attachEvent("onreadystatechange",H),e.attachEvent("onload",H);var r=!1;try{r=null==e.frameElement&&o.documentElement}catch(i){}r&&r.doScroll&&function a(){if(!b.isReady){try{r.doScroll("left")}catch(e){return setTimeout(a,50)}q(),b.ready()}}()}return n.promise(t)},b.each("Boolean Number String Function Array Date RegExp Object Error".split(" "),function(e,t){l["[object "+t+"]"]=t.toLowerCase()});function M(e){var t=e.length,n=b.type(e);return b.isWindow(e)?!1:1===e.nodeType&&t?!0:"array"===n||"function"!==n&&(0===t||"number"==typeof t&&t>0&&t-1 in

	e)}r=b(o);var _={};function F(e){var t=_[e]={};return b.each(e.match(w)||[],function(e,n){t[n]=!0}),t}b.Callbacks=function(e){ e="string"==typeof e?_[e]||F(e):b.extend({},e);var n,r,i,o,a,s,u=[],l=!e.once&&[],c=function(t){for(r=e.memory&&t,i=!0,a=s||0,s=0,o=u.length,n=!0;u&&o>a;a++)if(u[a].apply(t[0],t[1])===!1&&e.stopO nFalse){r=!1;break}n=!1,u&&(l?l.length&&c(l.shift()):r?u=[]:p.disable()) },p={add:function(){if(u){var t=u.length;(function i(t){b.each(t,function(t,n){var r=b.type(n);"function"===r?e.unique&&p.has(n)||u.push(n):n&&n.length&&"string"!==r&&i(n)})})(arguments),n?o=u.le ngth:r&&(s=t,c(r))}return this},remove:function(){return u&&b.each(arguments,function(e,t){var r;while((r=b.inArray(t,u,r))>-1)u.splice(r,1),n&&(o>=r&&o--,a>=r&&a--)}), this},has:function(e){return e?b.inArray(e,u)>-1:!(!u||!u.length)},empty: function(){return u=[],this},disable:function(){return u=l=r=t,this},disabled:function(){return!u},lock:function(){return l=t,r||p.disable(),this},locked:function(){return!l},fireWith:function(e, t){return t=t||[],t=[e,t.slice?t.slice():t],!u||i&&!l||(n?l.push(t):c(t)) ,this},fire:function(){return p.fireWith(this,arguments),this},fired:fun ction(){return!!i}};return p},b.extend({Deferred:function(e){var t=[["resolve","done",b.Callbacks("once memory"),"resolved"],["reject","fail",b.Callbacks("once memory"),"rejected"],["notif

4	ASP.NET版本泄露【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00137
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此Web应用程序返回的HTTP响应包括名为 X-AspNet-Version 的标头。 Visual Studio使用此标头的值来确定正在使用哪个版本的ASP.NET。 对于生产站点而言，这不是必需的，应该禁用。
风险影响	HTTP标头可能会泄露敏感信息。 此信息可用于发起进一步的攻击。
解决方案	对web.config文件应用以下更改以防止ASP.NET版本泄漏：<System.Web> <httpRuntime enable VersionHeader="false" /> </System.Web>
	举证描述： - 页面：http://www.th-storage.com 请求： GET /|~.aspx HTTP/1.1 Host: www.th-storage.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 500 Internal Server Error Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/7.5 X-AspNet-Version: 2.0.50727 Date: Wed, 19 Feb 2025 10:00:14 GMT Connection: keep-alive Content-Length: 2907 <html> <head> <title>运行时错误</title> <style> body {font-family:"Verdana";font-weight:normal;font

风险举证	-size: .7em;color:black;} p {font-family:"Verdana";font-weight:normal;co lor:black;margin-top: -5px} b {font-family:"Verdana";font-weight:bold;c o lor:black;margin-top: -5px} H1 { font-family:"Verdana";font-weight:nor ma l;font-size:18pt;color:red } H2 { font-family:"Verdana";font-weight:n orm al;font-size:14pt;color:maroon } pre {font-family:"Lucida Console";font-size: .9em} .marker {font-weight: bold; color: black;text-decoration: none;} .version {color: gray;} .error {margin-bottom: 10px;} .expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:hand; } </style> </head>

5	OPTIONS方法启用【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00126
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此Web服务器上启用了HTTP OPTIONS方法。 OPTIONS方法提供了Web服务器支持的方法列表，它表示对有关由Request-URI标识的请求/响应链上可用的通信选项的信息的请求。
风险影响	OPTIONS方法可能会公开敏感信息，这些信息可能有助于恶意用户准备更高级的攻击。
解决方案	建议在Web服务器上禁用OPTIONS方法。
风险举证	举证描述： - 页面：http://www.th-storage.com 请求： OPTIONS HTTP/1.1 Host: www.th-storage.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive Content-Length: 0 响应： HTTP/1.1 200 OK Allow: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/7.5 Public: OPTIONS, TRACE, GET, HEAD, POST Date: Wed, 19 Feb 2025 10:00:20 GMT Connection: keep-alive Content-Length: 0

6	general 未设置cookie的Secure标志位【原理扫描】
风险等级	低
深信服漏洞编号	SF-2016-00025
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	通用型(general)漏洞并不针对某一系统，其在各类系统中都有可能存在。Cookie Without Secure Flag Set是指服务器Set-Cookie消息头中未设置可选属性Secure，如果服务器设置这个属性，那么cookie只能在HTTPS请求中提交。

风险影响	影响所有Set-Cookie消息头中未设置可选属性Secure的系统
解决方案	为cookie设置Secure属性
风险举证	举证描述： - 页面：http://www.th-storage.com 请求： GET HTTP/1.1 Host: www.th-storage.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 404 Not Found Cache-Control: private Content-Length: 2320 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDACCDDDDD=JJDMNJMCJOEFGICFHMIGKLAK; path=/ Date: Wed, 19 Feb 2025 10:00:18 GMT Connection: keep-alive <!DOCTYPE html PUBLIC " -//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 网站访问报错</title> <style type="text/css"> * { padding:0; margin:0;} li { list-style:none;} img { border:none;} .clear { zoom:1;} . clear:after { content:'\20'; clear:both; display:block;}

7	Microsoft IIS版本泄露【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00136
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此web应用程序返回的HTTP响应包括名为Server的头。此头的值包括Microsoft IIS服务器的版本。
风险影响	HTTP头可能会泄漏敏感信息。这些信息可以进行发动进一步的攻击。
解决方案	Microsoft IIS应该配置为从响应中删除不需要的HTTP响应标头。 有关更多信息，请参考网络参考。
风险举证	举证描述： - 页面：http://www.th-storage.com 请求： GET HTTP/1.1 Host: www.th-storage.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 404 Not Found Cache-Control: private Content-Length: 2320 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDACCDDDDD=FLCMNJMCEPEMINHJHCNDFCKK; path=/ Date: Wed, 19 Feb 2025 10:00:14 GMT Connection: keep-alive <!DOCTYPE html PUBLIC " -//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 网站访问报错</title> <style type="text/css"> * { padding:0; margin:0;} li { list-style:none;} img { border:none;} .clear { zoom:1;} . clear:after { content:'\20'; clear:both; display:block;}

8	邮箱地址泄露【原理扫描】

风险等级	低
深信服漏洞编号	SF-0000-0367
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	一个或多个电子邮件地址在这个页面被发现。大部分垃圾邮件来自互联网上收集的电子邮件地址。垃圾邮件机器人(也被称为电子邮件收割机和电子邮件提取器)是一种程序，它可以在互联网上搜寻任何遇到的网站上的电子邮件地址。垃圾邮件机器人程序寻找像myname@mydomain.com这样的字符串，然后记录找到的任何地址。
风险影响	攻击者可以获取到邮箱地址，并向该地址发送垃圾邮件攻击
解决方案	修改源代码，避免返回敏感信息。
风险举证	举证描述： Pattern found: th-storage@thtf.com.cn 页面： http://www.th-storage.com/about.asp 请求： GET /about.asp HTTP/1.1 Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Cookie : ASPSESSIONIDAABABCCC=NBOLIHMCHPALEPLKMGKLBFIE; path=/ Upgrade-Insecure-Requests : 1 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36 响应： HTTP/1.1 200 OK Cache-Control : private Content-Length : 25102 Content-Type : text/html Date : Wed, 19 Feb 2025 11:31:16 GMT Server : Microsoft-IIS/7.5 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 招聘信息-北京同方光盘股份有限公司</title> <meta name="keywords" content="同方光盘,北京同方光盘股份有限公司"> <meta name="description" content="北京同方光盘股份有限公司作为同方股份有限公司全资子公司，注册资本4000万，是最早从事光存储安全与应用的高新技术企业之一，公司创立了国内第一家光盘自有品牌，是移动存储领域的专业制造商和光盘安全存储及恢复的专业服务商。"> <link href="css/css.css" rel="stylesheet" type="text/css" /> <link href="css/style.css" rel="stylesheet" type="text/css" /> <link href="css/pro.css" rel="stylesheet" type="text/css" /> <link rel="stylesheet" href="wei/reset.css" type="text/css" media="screen" charset="utf-8"> <script src="wei/jQuery.js" type="text/javascript" charset="utf-8"></script> <script src="wei/new.js" type="text/javascript" charset="utf-8"></script> </head> <body> <script> var _hmt = _hmt || []; (function() { var hm = document.createElement("script"); hm.src = "https://hm.baidu.com/hm.js?597805b8f3a912caaa0e90184d25abc0"; var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(hm, s); })(); </script> 欢迎您访问北京同方光盘股份有限公司，我们将竭诚为您服务！ 微信 <img src="wei/mallewm.jpg" width="108" alt="" class="poa dn"> <p

	style="text-align:right; padding-right:80px;">欢迎致电：010-62780307 / 82863225</p> <table cellspacing="0" cellpadding="0" width="220" align="right" border="0"> <tbody> </tbody> <form action="products.asp" method="post" name="search" id="search"> <tr> <td width="75%" align="left" valign="middle" background="images/index_04.jpg"><input id="k" name="k" size="17" maxlength="50" style="BORDER: #cccccc 0px solid;HEIGHT: 16px; BACKGROUND-COLOR: #9e9e9e; color:#FFFFFF" onfocus="if(this.value=='Search') this.value=''" onblur="if(this.value=='') this.value='Search'" value="Search"/></td> <td width="25%" align="left" valign="middle" ><input type="image" height="55" width="49" src="images/index_05.jpg" align="absmiddle" name="submit" /></td> </tr>
风险举证	</form> </table> <h3>首页</h3> <h3 class="see">产品中心</h3> 光盘 档案级 清华同方DVD档案级光盘 4.7G 清华同方BD蓝光档案级光盘（25G） 清华同方BD蓝光档案级光盘（50G） 清华同方BD蓝光档案级光盘128G（25片装） 专业级 清华同方专业级光盘 清华同方高光可打印DVD专业级光盘 4.7G 清华同方专业级BD25G光盘 清华同方高光可打印专业级BD25G光盘 消费级 清华同方CD 清华同方DVD光盘 A+级 清华同方DVD光盘 清华同方可打印DVD光盘 清华同方飞天DVD光盘 清华同方丝羽DVD光盘 清华同方水清DVD光盘 清华同方涅槃光盘 <a href="products.asp?cataid=176"

	class="dropRight">光盘刻录机 <a href="products
风险举证	.asp?cataid=219" class="dropRight">档案级光盘刻录机 专业级光盘刻录机 便携式刻录机 外置超薄DVD/CD刻录机 全自动打印刻录一体机 入门级 专业级DVD光盘打印刻录一体机 专业级BD光盘打印刻录一体机 档案级DVD光盘打印刻录一体机 档案级BD光盘打印刻录一体机 进阶级 专业级DVD光盘打印刻录一体机-100片 专业级BD光盘打印刻录一体机-100片 档案级DVD光盘打印刻录一体机-100片 档案级BD光盘打印刻录一体机-100片 高端级 档案级DVD光盘打印刻录一体机-150片 档案级BD光盘打印刻录一体机-150片 档案级DVD光盘打印刻录一体机-400片 档案级BD光盘打印刻录一体机-400片 归档光盘检测仪
风险举证	TH- 6800T 清华同方便携归档光盘检测仪TH- 6800T 全自动档案检测仪TF-20型 全自动档案检测仪 <a href="products.asp?

9	cookie 没有设置httponly标志位【原理扫描】
风险等级	低

深信服漏洞编号	SF-2021-00870
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	HttpOnly 主要是为了限制web页面程序的browser端script程序读取cookie，防止恶意代码获取客户的敏感信息。
风险影响	远程攻击者可以利用此漏洞获取敏感信息
解决方案	为SetCookie配置HttpOnly属性
风险举证	举证描述： - 页面：http://www.th-storage.com 请求： GET HTTP/1.1 Host: www.th-storage.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 404 Not Found Cache-Control: private Content-Length: 2320 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDACCDDDDD=JJDMNJMCJOEFGICFHMIGKLAK; path=/ Date: Wed, 19 Feb 2025 10:00:18 GMT Connection: keep-alive <!DOCTYPE html PUBLIC " -//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 网站访问报错</title> <style type="text/css"> * { padding:0; margin:0;} li { list-style:none;} img { border:none;} .clear { zoom:1;} .clear:after { content:'\20'; clear:both; display:block;}

5.2.3 弱口令

该资产不存在弱口令风险。

5.2.3 登录入口

该资产不存在登录入口风险。

5.3 http://th-info.com

5.3.1 系统漏洞

1	IIS FTPSVC远程拒绝服务漏洞(CVE-2010-3972)
风险等级	高
深信服漏洞编号	SF-0005-17606

CVE编号	CVE-2010-3972
CNNVD编号	CNNVD-201012-307
CNVD编号	
Bugtraq编号	45542
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。Windows 7 IIS 7.5处理请求中的Telnet协议转义时存在的堆溢出问题，远程可以利用此漏洞导致服务器程序崩溃，拒绝服务合法用户或导致执行任意代码。
风险影响	影响IIS:7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS11-004）以及相应补丁 MS11-004：Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-004
风险举证	IIS:7.5

2	IIS FastCGI请求头远程溢出漏洞(CVE-2010-2730)
风险等级	高
深信服漏洞编号	SF-0005-17607
CVE编号	CVE-2010-2730
CNNVD编号	CNNVD-201009-133
CNVD编号	CNVD-2010-2000
Bugtraq编号	43138
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。对于启用了FastCGI功能的IIS服务器，远程攻击者可以通过提交特制的HTTP请求触发缓冲区溢出，导致执行任意代码。
风险影响	影响IIS:7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS10-065）以及相应补丁 MS10-065：Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-065
风险举证	IIS:7.5

3	IIS 重复参数请求拒绝服务漏洞(CVE-2010-1899)
风险等级	中
深信服漏洞编号	SF-0005-17608
CVE编号	CVE-2010-1899
CNNVD编号	CNNVD-201009-126

CNVD编号	CNVD-2010-1985
Bugtraq编号	43140
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。IIS中的脚本处理代码在处理重复的参数请求时存在栈溢出漏洞，远程攻击者可以通过对IIS所承载网站的ASP页面发送特制URI请求来利用这个漏洞，导致服务崩溃。
风险影响	影响IIS:6.0版本,7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS10-065）以及相应补丁 MS10-065：Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-065
风险举证	IIS:7.5

5.3.2 web漏洞

1	跨站脚本漏洞【原理扫描】
风险等级	高
深信服漏洞编号	SF-0000-0361
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	跨站点脚本攻击(也称为XSS)是一个漏洞，它允许攻击者向另一个用户发送恶意代码(通常以Javascript的形式)。 因为浏览器无法知道脚本是否应该被信任，所以它将在用户上下文中执行脚本，允许攻击者访问浏览器保留的任何cookie或会话标记。
风险影响	恶意用户可能会将JavaScript、VBScript、ActiveX、HTML或Flash注入易受攻击的应用程序中，欺骗用户以收集数据。攻击者可以窃取会话cookie并冒充用户接管帐户。也可以修改呈现给用户的页面内容。
解决方案	过滤输入的用户参数
	举证描述： URL encoded POST input xuhao was set to 1<WZVXXR>VWVDU</WZVXXR> The input is reflected inside a text element. 页面：http://th-info.com/search.asp 请求： POST /search.asp HTTP/1.1 Referer: http://th-info.com/search.asp Connection: Keep-Alive Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Cookie: ASPSESSIONIDAABABCCC=MPLLIHMCKMNIONMMJFHHJNKB; path=/ Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36 Content-Type: application/x-www-form-urlencoded

<table>
<tr><td>风险举证</td><td>xuhao=1<WZVXXR>VWVDU%5B%21%2B%21%5D</WZVXXR>&button2=%E5%BC%80%E5%A7%8B%E6%9F%A5%E8%AF%A2&act=search 响应： HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html Content-Encoding: gzip Vary: Accept-Encoding Server: Microsoft-IIS/7.5 Date: Wed, 19 Feb 2025 11:16:06 GMT Content-Length: 7543 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title>□□□□□□□□□·□□□è□□_□□□□□□□□□□□□□□□□□ □□□□è□□□□□□□□□□é□□□ □□□□</title> <meta name="keywords" content="□□□□□□□□ □□□□,□□□□□□□□□□□□□□□□□ □□□□è□□□□□□□□□□é□□□ □□□□"> <meta name="description" content="□□□□□□□□□□□□□□□□ □□□□è□□□□□□□□□□é□□□ □□□□□□□□□□□□□□□□□□□□□è□□□□□□□□□□é□□□ □□□□□□ ¨è□□□□□□□ □□□□□□□□□□□¨□□□è□□□□□□4000□□□□□□□□□ □□□□□□□□□□□□□□□□□□□ □□□□□□□¨□□□□ ¨□□□□□□□□□□¨□□□é□□□□° □□□□□□□□□□□□□□□□□□□□□ □□□□□□ □□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□ □□□□è□□□□□□□□□□□□□□□□□□□□□□□□§□□□¨□□□□□□¨é□□ □□□□□□□□□□□□□□□□□□□□□é□ □□□□□□□□□ □□□□□□□□□□ ¨□□□□□□¨□□□□□□□□□¤□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □"> <link href="css/css.css" rel="stylesheet" type="text/css" /> <link href="css/style.css" rel="stylesheet" type="text/css" /> <link href="css/pro.css" rel="stylesheet" type="text/css" /> <link rel="stylesheet" href="wei/reset.css" type="text/css" media="screen" charset="utf-8"> <script src="wei/jQuery.js" type="text/javascript" charset="utf-8"></script> <script src="wei/new.js" type="text/javascript" charset="utf-8"></script> </head> <body> <script> var _hmt = _hmt || []; (function() { var hm = document.createElement("script"); hm.src = " https://hm.baidu.com/hm.js?597805b8f3a912caaa0e90184d25abc0"; var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(hm, s); })(); </script> <div id="top"> <div class="w1180"> <div class="c1"> <div class="d1">□□□è□□□□¨è□□é□□□□□□□□□□□□□□□□□□ □□□□è□□□□□□□□□□é□□□ □□□□□□□□□□□□□□□□□° □□□□è □□□□□□□□□¨□□□□□□□□□□□</div> <div class="d2"> <div class="n-htop por z2"> <div class="m fr por curp"> □□□□□□□ <img src="wei/mallewm.jpg" width="108" alt="" class="poa dn"> </div> <p style="text-align:right; padding-right:80px;">□□□è□□è□□□□□□□□□010-62780307 / 82863225</p> </div> </div> <div class="d3"> <table cellspacing="0" cellpadding="0" width="220" align="right" border="0"> <tbody> </tbody> <form acti</td></tr>
<tr><td></td><td>on="products.asp" method="post" name="search" id="search"> <tr> <td width="75%" align="left" valign="middle" background="images/index_04.jpg"><input id="k" name="k" size="17" maxlength="50" style="BORDER: #cccccc 0px solid;HEIGHT: 16px; BACKGROUND-COLOR: #9e9e9e; color:#FFFFFF" onfocus="if(this.value=='Search') this.value=''" onblur="if(this.value=='') this.value='Search'" value="Search"/></td> <td width="25%" align="left" valign="middle" ><input type="image"</td></tr>
</table>

风险举证	height="55" width="49" src="images/index_05.jpg" align="absmiddle" name="submit" /></td> </tr> </form> </table> </div> </div> <div class="headerr "> <div class="wrap"> <div class="js-logo"></div> <h3>é□□é□□</h3> <h3 class="see">□□§□□□□□□□□□</h3> □ □□□□ □□□□□□□□§ □□ □□□□□□□□□DVD□□□□□□□□§□ □□□□□ 4.7G □□ □□□□□□□□□BDè□□□ □□□□□□□□□§□ □□□□□□□25G□□□ □□ □□□□□□□□□BDè□□□ □□□□□□□□□§□ □□□□□□□50G□□□ □□ □□□□□□□□□BDè□□□ □□□□□□□□□§□ □□□□128G□□□25□□□è□ □□□ □□□□□□□□§ □□ □□□□□□□□□□□□□□□□□§□ □□□□ □□ □□□□□□□□□é□□□ □□□□□□□□□° DVD□□□□□□□□§□ □□□□4.7G □□ □□□□□□□□□□□□□□□□□§BD25G□ □□□□ □□ □□□□□□□□□é□□□ □□□□□□□□□° □□□□□□□□§BD25G□ □□□□ □□□è□□□□§ □□ □□□□□□□□□CD □□ □□□□□□□□□DVD□ □□□□ A+□□§ <a href="products_detai
风险举证	l.asp?id=1050">□□ □□□□□□□□□DVD□ □□□□ □□ □□□□□□□□□□□□□□□□□° DVD□ □□□□ □□ □□□□□□□□□é□□□¤□DVD□ □□□□ □□ □□□□□□□□□□□□□□□DVD□ □□□□ □□ □□□□□□□□□□° □□□ DVD□ □□□□ □□ □□□□□□□□□□□ □§□□ □□□□ □ □□□□□□□□□□□□□ □□□□□□□□§□ □□□□□□□□□□□□□ □□□□□□□□§□ □□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□ □¤□□□□è□ è□□DVD/CD□□□□□□□□□ □

	¨è□□□□¨□□□□□°□□□□□□□□□□□□□□□□ □ □é□¨□□§ □□□□□□□□§DVD□□□□□□□□□°□□□□□□□□□□□□□□□□ □□□□□□□□§BD□□□□□□□□□°□□□□□□□□□□□□□□□□ □□□□□□□□§DVD□□□□□□□□□°□□□□□□□□□□□□□□□□ □□□□□□□□§BD□□□□□□□□□°□□□□□□□□□□□□□□□□ è□□é□□□□§ □□□□□□□□§DVD□□□□□□□□□°□□□□□□□□□□□□□□□□-100□□□ □□□□□□□□§BD□□□□□□□□□°□□□□□□□□□□□□□□□□-100□□□
风险举证	□□□□□□□□§DVD□□□□□□□□□°□□□□□□□□□□□□□□□□-100□□□ □□□□□□□□§BD□□□□□□□□□°□□□□□□□□□□□□□□□□-100□□□ é□□□□□□□§ □□□□□□□□§DVD□□□□□□□□□°□□□□□□□□□□□□□□□□-150□□□ □□□□□□□□§BD□□□□□□□□□°□□□□□□□□□□□□□□□□-150□□□ □□□□□□□□§DVD□□□□□□□□□°□□□□□□□□□□□□□□□□-400□□□ <l

2	SQL注入攻击【原理扫描】
风险等级	高
深信服漏洞编号	SF-0000-0378
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	该网站可能易受SQL注入攻击。 SQL注入漏洞允许攻击者通过操纵用户输入改变后端SQL语句。若Web应用程序收到用户输入时直接放入SQL语句，而没有正确过滤危险字符时，会发生SQL注入。
风险影响	攻击者可以在受害网站上执行任意SQL语句。可能会破坏数据库的完整性或暴露敏感信息。甚至执行shell命令，威胁整个网站服务器。
解决方案	严格过滤用户输入的数据。
	举证描述： URL encoded GET input id was set to 401/(3*2-5) Tests performed: ,,,,, Original value: 401 页面：

风险举证	http://th-info.com/faq_detail.asp?id=401 请求： GET /faq_detail.asp?id=401/(3*2-5) HTTP/1.1 X-Requested-With: XMLHttpRequest Referer: http://th-info.com/faq_detail.asp?id=401 Connection: Keep-Alive Cookie: ASPSESSIONIDAABABCCC=MPLLIHMCKMNIONMMJFHH JNKB; path=/ User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 响应： HTTP/1.1 200 OK Cache-Control: private Content-Length: 30828 Content-Type: text/html Server: Microsoft-IIS/7.5 Date: Wed, 19 Feb 2025 11:32:11 GMT <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-tran sitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title>□□□□□□□□§□ □□□□□□□□□□□□□¨□□□□□□é□□_ □□□□□□□□□□□□□ □□□□è□□□□□□□□é□□□ □□□□</title> <meta name="keywords" content="□□□□□□□ □□□□,□□□□□□□□□□□□□ □□□□è□□□□□□□□é□□□ □□□□"> <meta name="description" content="□□□□□□□□□□□□□ □□□□è□□□□□□□□é□□□ □□□□□□□□□□□□□□□□è□□□ □□□□□é□□□ □□□□□ ¨è□□□□□□ □□□□□□□□□¨□□□è□□□□□4000□□□□□□□□□□□□□□□ □□□□□□□ □□□□□□¨□□□□ ¨□□□□□□□¨□□□é□□□ □° □□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□ □□□□□□□□□□□ □□□□è□□□□□□□□□□□□□□□□§□□□¨□□□□□¨é□□ □□□□□□□□□□□□□□□□é□ □□□□□□□ □□□□□□□□ ¨□□□□□¨□□□□□□□¤□□□□□□□□□□□□□□□□□□□□ □"> <link href="css/css.css" rel="stylesheet" type="text/css" /> <link href="css/style.css" rel="stylesheet" type="text/css" /> <link href="css/pro.css" rel="stylesheet" type="text/css" /> <link rel="stylesheet" href="wei/reset.css" type="text/css" media="screen" charset="utf-8"> <script src="wei/jQuery.js" type="text/javascript" charset="utf-8"></script> <script src="wei/new.js" type="text/javascript" charset="utf-8"></script> </head> <body> <script> var _hmt = _hmt || []; (function() { var hm = document.createElement("script"); hm.src = " https://hm.baidu.com/hm.js?597805b8f3a912caaa0e90184d25abc0"; var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(hm, s); })(); </script> □□□è□□□□¨è□□é□□□□□□□□□□□□□□□ □□□□è□□□□□□□□é□□□ □□□□□□□□□□□□□□□° □□□□è □□□□□□□¨□□□□□□□□□ □□□□□□ <img src="wei/mallewm.jpg" width="108" alt="" class="poa dn"> □□□è□□è□□□□□□□□010-62780307 / 82863225 <table cellspacing="0" cellpadding="0" width="220" align="right" border="0"> <tbody> </tbody> <form action="products.asp" method="post" name="search" id="search"> <tr> <td width="75%" align="left" valign="middle" background="images/index_04.jpg"><input id="k" name="k" size="17" maxlength="50" style="BORDER: #cccccc 0px solid;HEIGHT: 16px;

	BACKGROUND-COLOR: #9e9e9e; color:#F

风险举证	FFFFF" onfocus="if(this.value=='Search') this.value=''" onblur="if(this.value=='') this.value='Search'" value="Search"/></td> <td width="25%" align="left" valign="middle" ><input type="image" height="55" width="49" src="images/index_05.jpg" align="absmiddle" name="submit" /></td> </tr> </form> </table> <h3>é□□é□□</h3> <h3 class="see">□□§□□□□□□□□□</h3> □□□□□ □□□□□□□□§ □□ □□□□□□□□□DVD□□□□□□□□§□ □□□□□ 4.7G □□ □□□□□□□□□BDè□□□ □□□□□□□□□§□ □□□□□□□25G□□□ □□ □□□□□□□□□BDè□□□ □□□□□□□□□§□ □□□□□□□50G□□□ □□ □□□□□□□□□BDè□□□ □□□□□□□□□§□ □□□□128G□□□25□□□è□ □□□ □□□□□□□□§ □□ □□□□□□□□□□□□□□□□□□§□ □□□□ □□ □□□□□□□□□é□□□ □□□□□□□□□° DVD□□□□□□□□§□ □□□□4.7G □□ □□□□□□□□□□□□□□□□□§BD25G□ □□□□ □□ □□□□□□□□□é□□□ □□□□□□□□□° □□□□□□□□§BD25G□ □□□□ □□□è□□□□§ □□ □□□□□□□□□CD □□ □□□□□□□□□DVD□ □□□□ A+□□§ □□ □□□□□□□□□DVD□ □□□□ □□ □□□□□□□□□□□□□□□□□□° DVD□ □□□□ □□ □□□□□□□□□é□□□¤□DVD□ □□□□
	□□ □□□□□□□□□□□□□□□□DVD□ □□□□ □□ □□□□□□□□□□° □□□ DVD□ □□□□ □□ □□□□□□□□□□□ □§□□ □□□□ □□□□□□□□□□□□□□□ □□□□□□□§□ □□□□□□□□□□□□□□ □□□□□□□§□ □□□□□□□□□□□□□□ <a href="products.asp?cataid=231"

风险举证	class="dropRight">□□□□□□□□□□□□□□□□□□□ □¤□□□□è□ è□□DVD/CD□□□□□□□□□□□ □ ¨è□□□□¨□□□□□°□□□□□□□□□□□□□□□□□ □ □é□¨□□§ □□□□□□□□§DVD□ □□□□□□□□□°□□□□□□□□□□□□□□□□□ □□□□□□□□§BD□ □□□□□□□□□°□□□□□□□□□□□□□□□□□ □□□□□□□□§DVD□ □□□□□□□□□°□□□□□□□□□□□□□□□□□ □□□□□□□□§BD□ □□□□□□□□□°□□□□□□□□□□□□□□□□□ è□□é□□□□§ □□□□□□□□§DVD□ □□□□□□□□□°□□□□□□□□□□□□□□□□-100□□□ □□□□□□□□§BD□ □□□□□□□□□°□□□□□□□□□□□□□□□□-100□□□ □□□□□□□□§DVD□ □□□□□□□□□°□□□□□□□□□□□□□□□□-100□□□ □□□□□□□□§BD□ □□□□□□□□□°□□□□□□□□□□□□□□□□-100□□□ <
风险举证	/ul> é□□□□□□□§ □□□□□□□□§DVD□ □□□□□□□□□°□□□□□□□□□□□□□□□□-150□□□ □□□□□□□□§BD□ □□□□□□□□□°□□□□□□□□□□□□□□□□-150□□□ □□□□□□□□§DVD□ □□□□□□□□□°□□□□□□□□□□□□□□□□-400□□□

3	Javascript库不安全【原理扫描】
风险等级	中
深信服漏洞编号	SF-0000-0382
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	正在使用易受攻击的Javascript库。 已报告此版本的Javascript库存在一个或多个漏洞。 有关受影响的库和所报告的漏洞的更多信息，请查阅攻击详细信息和Web参考。
风险影响	有关更多信息，请参考Web参考。
解决方案	升级到最新版本。

风险举证	举证描述： Detected Javascript library jquery version 1.4.2. The version was detected from name, and contents, and contents. 页面： http://th-info.com/pro/jquery-1.4.2.js 请求： GET /pro/jquery-1.4.2.js HTTP/1.1 Accept : */* Referer : http://th-info.com/products.asp?cataid=194 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36 响应： HTTP/1.1 200 OK Content-Type : application/x-javascript Content-Encoding : gzip Last-Modified : Mon, 31 Oct 2016 12:48:34 GMT Accept-Ranges : bytes ETag : "03d2a177533d21:0" Vary : Accept-Encoding Server : Microsoft-IIS/7.5 Date : Wed, 19 Feb 2025 10:38:47 GMT Content-Length : 46482/*! * jQuery JavaScript Library v1.4.2 * http://jquery.com/ * * Copyright 2010, John Resig * Dual licensed under the MIT or GPL Version 2 licenses. * http://jquery.org/license * * Includes Sizzle.js * http://sizzlejs.com/ * Copyright 2010, The Dojo Foundation * Released under the MIT, BSD, and GPL Licenses. * * Date: Sat Feb 13 22:33:48 2010 -0500 */ (function(window, undefined) { // Define a local copy of jQuery var jQuery = function(selector, context) { // The jQuery object is actually just the init constructor 'enhanced' return new jQuery.fn.init(selector, context); }, // Map over jQuery in case of overwrite _jQuery = window.jQuery, // Map over the $ in case of overwrite _$ = window.$, // Use the correct document accordingly with window argument (sandbox) document = window.document, // A central reference to the root jQuery(document) rootjQuery, // A simple way to check for HTML strings or ID strings // (both of which we optimize for) quickExpr = /^[^<]*(<[\w\W]+>)[^>]*$|^#([\w-]+)$/, // Is it a simple selector isSimple = /^.[^:#\[\.,]*$/, // Check if a string has a non-whitespace character in it rnotwhite = /\S/, // Used for trimming whitespace rtrim = /^(\s|\u00A0)+|(\s|\u00A0)+$/g, // Match a standalone tag rsingleTag = /^<(\w+)\s*\/?>(?:<\/\1>)?$/, // Keep a UserAgent string for use with jQuery.browser userAgent = navigator.userAgent, // For matching the engine and version of the browser browserMatch, // Has the ready events already been bound? readyBound = false, // The functions to execute on DOM ready readyList = [], // The ready event handler DOMContentLoaded, // Save a reference to some core methods toString = Object.prototype.toString, hasOwnProperty = Object.prototype.hasOwnProperty, push = Array.prototype.push, slice = Array.prototype.slice, indexOf = Array.prototype.indexOf; jQuery.fn = jQuery.prototype = { init: function(selector, context) { var match, elem, ret, doc; // Handle $(""), $(null), or $(undefined) if (!selector) { return this; } // Handle $(DOMElement) if (selector.nodeType) { this.context = this[0] = selector; this.length = 1; return this; } // The body element only exists once, optimize finding it if (selector === "body" && !context) { this.context = document; this[0] = document.body; this.selector = "body"; this.length = 1; return this; } // Handle HTML strings if (typeof selector === "string") { // Are we dealing with HTML string or an ID? match = quickExpr.exec(selector); // Verify a match, and that n
	o context was specified for #id if (match && (match[1] || !context)) { // HANDLE: $(html) -> $(array) if (match[1]) { doc = (context ? context.ownerDocument || context : document); // If a single string is passed in and it's a single tag // just do a createElement and skip the rest ret = rsingleTag.exec(selector); if (ret) { if (jQuery.isPlainObject(context)) { selector = [

风险举证	document.createElement(ret[1])]; jQuery.fn.attr.call(selector, context, true); } else { selector = [doc.createElement(ret[1])]; } } else { ret = buildFragment([match[1]], [doc]); selector = (ret.cacheable ? ret.fragment.cloneNode(true) : ret.fragment).childNodes; } return jQuery.merge(this, selector); // HANDLE: $("#id") } else { elem = document.getElementById(match[2]); if (elem) { // Handle the case where IE and Opera return items // by name instead of ID if (elem.id !== match[2]) { return rootjQuery.find(selector); } // Otherwise, we inject the element directly into the jQuery object this.length = 1; this[0] = elem; } this.context = document; this.selector = selector; return this; } // HANDLE: $("TAG") } else if (!context && /^\w+$/.test(selector)) { this.selector = selector; this.context = document; selector = document.getElementsByTagName(selector); return jQuery.merge(this, selector); // HANDLE: $(expr, $(...)) } else if (!context || context.jquery) { return (context || rootjQuery).find(selector); // HANDLE: $(expr, context) // (which is just equivalent to: $(context).find(expr) } else { return jQuery(context).find(selector) ; } // HANDLE: $(function) // Shortcut for document ready } else if (jQuery.isFunction(selector)) { return rootjQuery.ready(selector); } if (selector.selector !== undefined) { this.selector = selector.selector; this.context = selector.context; } return jQuery.makeArray(selector, this); }, // Start with an empty selector selector: "", // The current version of jQuery being used jquery: "1.4.2", // The default length of a jQuery object is 0 length: 0, // The number of elements contained in the matched element set size: function() { return this.length; }, toArray: function() { return slice.call(this, 0); }, // Get the Nth element in the matched element set OR // Get the whole matched element set as a clean array get: function(num) { return num == null ? // Return a 'clean' array this.toArray() : // Return just the object (num < 0 ? this.slice(num)[0] : this[num]); }, // Take an array of elements and push it onto the stack // (returning the new matched element set) pushStack: function(elems, name, selector) { // Build a new jQuery matched element set var ret = jQuery(); if (jQuery.isArray(elems)) { push.apply(ret, elems); } else { jQuery.merge(ret, elems); } // Add the old object onto the stack (as a reference) ret.prevObject = this; ret.context = this.context; if (name === "find") { ret.selector = this.selector + (this.selector ? " " : "") + selector;
	} else if (name) { ret.selector = this.selector + "." + name + "(" + selector + ")"; } // Return the newly-formed element set return ret; }, // Execute a callback for every element in the matched set. // (You can seed the arguments with an array of args, but this is // only used internally.) each: function(callback, args) { return jQuery.each(this, callback, args); }, ready: function(fn) { // Attach the listeners jQuery.bindReady(); // If the DOM is already ready if (jQuery.isReady) { // Execute the function immediately fn.call(document, jQuery); // Otherwise, remember the function for later } else if (readyList) { // Add the function to the wait list readyList.push(fn); } return this; }, eq: function(i) { return i === -1 ? this.slice(i) : this.slice(i, +i + 1); }, first: function() { return this.eq(0); }, last: function() { return this.eq(-1); }, slice: function() { return this.pushStack(slice.apply(this,

风险举证	arguments), "slice", slice.call(arguments).join(",")); }, map: function(callback) { return this.pushStack(jQuery.map(this, function(elem, i) { return callback.call(elem, i, elem); })); }, end: function() { return this.prevObject || jQuery(null); }, // For internal use only. // Behaves like an Array's method, not like a jQuery method. push: push, sort: [].sort, splice: [].splice }; // Give the init function the jQuery prototype for later instantiation jQuery.fn.init.prototype = jQuery.fn; jQuery.extend = jQuery.fn.extend = function() { // copy reference to target object var target = arguments[0] || {}, i = 1, length = arguments.length, deep = false, options, name, src, copy; // Handle a deep copy situation if (typeof target === "boolean") { deep = target; target = arguments[1] || {}; // skip the boolean and the target i = 2; } // Handle case when target is a string or something (possible in deep copy) if (typeof target !== " object" && !jQuery.isFunction(target)) { target = {}; } // extend jQuery itself if only one argument is passed if (length === i) { target = this; --i; } for (; i < length; i++) { // Only deal with non-null/undefined values if ((options = arguments[i]) != null) { // Extend the base object for (name in options) { src = target[name] ; copy = options[name]; // Prevent never-ending loop if (target === copy) { continue; } // Recurse if we're merging object literal values or arrays if (deep && copy && (jQuery.isPlainObject(copy) || jQuery.isArray(copy))) { var clone

4	Javascript库不安全【原理扫描】
风险等级	中
深信服漏洞编号	SF-0000-0382
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	正在使用易受攻击的Javascript库。 已报告此版本的Javascript库存在一个或多个漏洞。 有关受影响的库和所报告的漏洞的更多信息，请查阅攻击详细信息和Web参考。
风险影响	有关更多信息，请参考Web参考。
解决方案	升级到最新版本。
	举证描述： Detected Javascript library jquery version 1.9.1. The version was detected from contents, and contents. 页面： http://th-info.com/./wei/jQuery.js 请求： GET /./wei/jQuery.js HTTP/1.1 Cookie : ASPSESSIONIDAABABCCC=NPLLIHMCKKKIFECMFJLOBKBM;HMACCOUNT_BFESS=D469E9ECADD76BC9;Hm_lvt_597805b8f3a912caaa0e90184d25abc0=1739961197;Hm_lpvt_597805b8f3a912caaa0e90184d25abc0=1739961197;HMACCOUNT=D469E9ECADD76BC9;__bid_n=1951dc4ee0421925a3531c;BAIDUID_BFESS=44A05949516BEA7CFD7B7E3DC9B8F67F:FG=1;sajssdk_2015_cross_new_user=1;sensorsdata2015jssdkcross=%7B%22distinct_id%22%3A%221951dc4ef142cd-09dbf86a314dbf8-26021a51-921600-1951dc4ef1598c%22%2C%22first_id%22%3A%22%22%2C%22props%22%3A%7B%22%24latest_traffic_source_type%22%3A%22%E7%9B%B4%E6%8E%A5%E6%B5%81%E9%87%8F%22%2C

风险举证	%22%24latest_search_keyword%22%3A%22%E6%9C%AA%E5%8F%96%E5%88%B0%E5%80%BC_%E7%9B%B4%E6%8E%A5%E6%89%93%E5%BC%80%22%2C%22%24latest_referrer%22%3A%22%7D%2C%22identities%22%3A%22eyIkaWRIbnRpdHIfY29va2IIX2IkIjoiMTk1MWRj NGVmMTQyY2QtMDIkYmY4NmEzMTRkYmY4LTI2MDIxYTUxLTkyMTYwMC0xOTUxZGM0ZWYxNTk4 YyJ9%22%2C%22history_login_id%22%3A%7B%22name%22%3A%22%22%2C%22value%22% 3A%22%22%7D%2C%22%24device_id%22%3A%221951dc4ef142cd-09dbf86a314dbf8-260 21a51-921600-1951dc4ef1598c%22%7D;Hm_lvt_597805b8f3a912caaa0e90184d25abc 0=1739961217;HMACCOUNT=D469E9ECADD76BC9;sajssdk_2015_cross_new_user=1;se nsorsdata2015jssdkcross=%7B%22distinct_id%22%3A%221951dc5763a159-0f893c5 48f8e81-26021a51-921600-1951dc5763bc55%22%2C%22first_id%22%3A%22%22%2C%2 2props%22%3A%7B%22%24latest_traffic_source_type%22%3A%22E7%9B%B4%E6%8E% A5%E6%B5%81%E9%87%8F%22%2C%22%24latest_search_keyword%22%3A%22%E6%9C%AA% E5%8F%96%E5%88%B0%E5%80%BC_%E7%9B%B4%E6%8E%A5%E6%89%93%E5%BC%80%22%2C%22 %24latest_referrer%22%3A%22%22%7D%2C%22identities%22%3A%22eyIkaWRIbnRpdH IfY29va2IIX2IkIjoiMTk1MWRjNTc2M2ExNTktMGY4OTNjNTQ4ZjhlODEtMjYwMjFhNTEtOT IxNjAwLTE5NTFkYzU3NjNiYzU1In0%3D%22%2C%22history_login_id%22%3A%7B%22nam e%22%3A%22%22%2C%22value%22%3A%22%22%7D%2C%22%24device_id%22%3A%221951dc 5763a159-0f893c548f8e81-26021a51-921600-1951dc5763bc55%22%7D;__bid_n=195 1dc5770174727ba8b59;ASPSESSIONIDAABABCCC=CIMLIHMCPLEJALLECBCALBMJ;Hm_lpv t_597805b8f3a912caaa0e90184d25abc0=1739961559 User-Agent : Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 响应： HTTP/1.1 200 OK Content-Type : application/x-javascript Content-Encoding : gzip Last-Modified : Wed, 20 Sep 2017 06:04:10 GMT Accept-Ranges : bytes ETag : "0a98846d631d31:0" Vary : Accept-Encoding Server : Microsoft-IIS/7.5 Date : Wed, 19 Feb 2025 11:36:44 GMT Content-Length : 32837/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license */(function(e,t){var n,r,i=typeof t,o=e.document,a=e.location,s=e.jQuery,u=e.$,l={},c=[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,g=c.indexOf,m=l.toString,y=l.hasOwnProperty,v=p.trim,b=function(e,t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,w=/\S+/g,T=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:(<[\w\W]+>)[^>]*|#([\w-]*))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,k=/^[\],:{}\s]*$/,E=/(?:^|:|,)(?:\s*\[)+/g,S=/\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,A=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^-ms-/,D=/-([\da-z])/gi,L=function(e,t){return t.toUpperCase()},H=function(e){(o.addEventListener||"load"===e.type||"complete"===o.readyState)&&(q(),b.ready()) },q=function(){o.addEventListener?(o.removeEventListener("
	DOMContentLoaded",H,!1),e.removeEventListener("load",H,!1)):(o.detachEvent("onreadystatechange",H),e.detachEvent("onload",H))};b.fn=b.prototype={jquery:p,constructor:b,init:function(e,n,r){var i,a;if(!e)return this;if("string"==typeof e){if(i="<"===e.charAt(0)&&">"===e.charAt(e.length-1)&&e.length>=3?[null,e,null]:N.exec(e),!i||!i[1]&&n)return!n||n.jquery?(n||r).find(e):this.constructor(n).find(e);if(i[1]){if(n=n instanceof b?n[0]:n,b.merge(this,b.parseHTML(i[1],n&&n.nodeType?n.ownerDocument||n:o,!0)),C.test(i[1])&&b.isPlainObject(n))for(i in n)b.isFunction(this[i])?this[i](n[i]):this.attr(i,n[i]);return this}if(a=o.getElementById(i[2]),a&&a.parentNode){if(a.id!==i[2])return r.find(e);this.length=1,this[0]=a}return this.context=o,this.selector=e,this}return e.nodeType?(this.context=this[0]=e,this.length=1,this):b.isFunction(e)?r.ready(e):(e.selector!==t&&(this.selector=e.selector,this.context=e.conte

风险举证	xt),b.makeArray(e,this))},selector:"",length:0,size:function(){return this.length},toArray:function(){return h.call(this)},get:function(e){return null==e?this.toArray():0>e?this[this.length+e]:this[e]},pushStack:function(e){var t=b.merge(this.constructor(),e);return t.prevObject=this,t.context=this.context,t},each:function(e,t){return b.each(this,e,t)},ready:function(e){return b.ready.promise().done(e),this},slice:function(){return this.pushStack(h.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-1)},eq:function(e){var t=this.length,n=+e+(0>e?t:0);return this.pushStack(n>=0&&t>n?[this[n]]:[])},map:function(e){return this.pushStack(b.map(this,function(t,n){return e.call(t,n,t)}))},end:function(){return this.prevObject||this.constructor(null)},push:d,sort:[].sort,splice:[].splice},b.fn.init.prototype=b.fn,b.extend=b.fn.extend=function(){var e,n,r,i,o,a,s=arguments[0]||{},u=1,l=arguments.length,c=!1;for("boolean"==typeof s&&(c=s,s=arguments[1]||{},u=2),"object"==typeof s||b.isFunction(s)||(s={}),l===u&&(s=this,--u);l>u;u++)if(null!=(o=arguments[u]))for(i in o)e=s[i],r=o[i],s!==r&&(c&&r&&(b.isPlainObject(r)||(n=b.isArray(r)))?(n?(n=!1,a=e&&b.isArray(e)?e:[]):a=e&&b.isPlainObject(e)?e:{},s[i]=b.extend(c,a,r)):r!==t&&(s[i]=r));return s},b.extend({noConflict:function(t){return e.$===b&&(e.$=u),t&&e.jQuery===b&&(e.jQuery=s),b},isReady:!1,readyWait:1,holdReady:function(e){e?b.readyWait++:b.ready(!0)},ready:function(e){if(e===!0?!--b.readyWait:!b.isReady){if(!o.body)return setTimeout(b.ready);b.isReady=!0,e!==!0&&--b.readyWait>0||(n.resolveWith(o,[b]),b.fn.trigger&&b(o).trigger("ready").off("ready"))}},isFunction:function(e){return"function"===b.type(e)},isArray:Array.isArray||function(e){return"array"===b.type(e)},isWindow:function(e){return null!=e&&e==e.window},isNumeric:function(e){return!isNaN(parseFloat(e))&&isFinite(e)},type:function(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[m.call(e)]||"object":typeof e},isPlainObject:function(e){if(!e||"object"!==b.type(e)||e.nodeType||b.isWindow(e))return!1;try{if(e.constructor&&!y.call(e,"constructor")&&!y.call(e.constructor.prototype,"isPrototypeOf"))return!1}catch(n){return!1}var r;for(r in e);return r===t||y.call(e,r)},isEmptyObject:function(e){var t;for(t in e)return!1;return!0},error:function(e){throw Error(e)},pa
	rseHTML:function(e,t,n){if(!e||"string"!=typeof e)return null;"boolean"==typeof t&&(n=t,t=!1),t=t||o;var r=C.exec(e),i=!n&&[];return r?[t.createElement(r[1])]:(r=b.buildFragment([e],t,i),i&&b(i).remove(),b.merge([],r.childNodes))},parseJSON:function(n){return e.JSON&&e.JSON.parse?e.JSON.parse(n):null===n?n:"string"==typeof n&&(n=b.trim(n),n&&k.test(n.replace(S,"@").replace(A,"]").replace(E,"")))?Function("return "+n)():(b.error("Invalid JSON: "+n),t)},parseXML:function(n){var r,i;if(!n||"string"!=typeof n)return null;try{e.DOMParser?(i=new DOMParser,r=i.parseFromString(n,"text/xml")):(r=new ActiveXObject("Microsoft.XMLDOM"),r.async="false",r.loadXML(n))}catch(o){r=t}return r&&r.documentElement&&!r.getElementsByTagName("parsererror").length||b.error("Invalid XML: "+n),r},noop:function(){},globalEval:function(t){t&&b.trim(t)&&(e.execScript||function(t){e.eval.call(e,t)})(t)},camelCase:function(e){return e.replace(j,"ms-").replace(D,L)},nodeName:function(e,t){return

风险举证	e.nodeName&&e.nodeName.toLowerCase()===t.toLowerCase()},each:function(e, t,n){var r,i=0,o=e.length,a=M(e);if(n){if(a){for(;o>i;i++)if(r=t.apply(e [i],n),r===!1)break}else for(i in e)if(r=t.apply(e[i],n),r===!1)break} el se if(a){for(;o>i;i++)if(r=t.call(e[i],i,e[i]),r===!1)break}else for(i in e)if(r=t.call(e[i],i,e[i]),r===!1)break;return e},trim:v&&!v.call("\ufeff\u00a0")?function(e){return null==e?"":v.call(e)}:function(e){return null==e?"":(e+"").replace(T,"")},makeArray:function(e,t){var n=t||[];return null!=e&&(M(Object(e))?b.merge(n,"string"==typeof e?[e]:e):d.call(n,e)),n},inArray:function(e,t,n){var r;if(t){if(g)return g.call(t,e,n);for(r=t.length,n=n?0>n?Math.max(0,r+n): n:0;r>n;n++)if(n in t&&t[n]===e)return n}return-1},merge:function(e,n){var r=n.length,i=e.length,o=0;if("number" ==typeof r)for(;r>o;o++)e[i++]=n[o];else while(n[o]!==t)e[i++]=n[o++];return e.length=i,e},grep:function(e,t,n){v ar r,i=[],o=0,a=e.length;for(n=!!n;a>o;o++)r=!!t(e[o],o),n!==r&&i.push(e [o]);return i},map:function(e,t,n){var r,i=0,o=e.length,a=M(e),s=[];if(a)for(;o>i;i++)r=t(e[i],i,n),null!=r&&(s [s.length]=r);else for(i in e)r=t(e[i],i,n),null!=r&&(s[s.length]=r);re t urn f.apply([],s)},guid:1,proxy:function(e,n){var r,i,o;return"string"==typeof n&&(o=e[n],n=e,e=o),b.isFunction(e)?(r=h.ca ll(arguments,2),i=function(){return e.apply(n||this,r.concat(h.call(arg u ments)))},i.guid=e.guid=e.guid||b.guid++,i):t},access:function(e,n,r,i, o, a,s){var u=0,l=e.length,c=null==r;if("object"===b.type(r)){o=!0;for(u in r)b.access(e,n,u,r[u],!0,a,s)}else if(i!==t&&(o=!0,b.isFunction(i)||(s=!0),c&&(s?(n.call(e,i),n=null):(c=n, n=function(e,t,n){return c.call(b(e),n)})),n))for(;l>u;u++)n(e[u],r,s?i: i.call(e[u],u,n(e[u],r)));return o?e:c?n.call(e):l?n(e[0],r):a},now:fun c tion(){return(new Date).getTime()}}),b.ready.promise=function(t){if(!n) i f(n=b.Deferred(),"complete"===o.readyState)setTimeout(b.ready);else if(o.addEventListener)o.addEventListener("DOMContentLoaded",H,!1),e.addE ventListener("load",H,!1);else{o.attachEvent("onreadystatechange",H),e. a ttachEvent("onload",H);var r=!1;try{r=null==e.frameElement&&o.document El ement}catch(i){}r&&r.doScroll&&function a(){if(!b.isReady){try{r.doScroll("left")}catch(e){return setTimeout(a,50)}q(),b.ready()}}()}return n.promise(t)},b.each("Boolean Number String Function Array Date
风险举证	RegExp Object Error".split(" "),function(e,t){l["[object " +t+"]"]=t.toLowerCase()});function M(e){var t=e.length,n=b.type(e);return b.isWindow(e)?!1:1===e.nodeType&&t?!0:"arr ay"===n||"function"!==n&&(0===t||"number"==typeof t&&t>0&&t-1 in e)}r=b(o);var _={};function F(e){var t=_[e]={};return b.each(e.match(w)||[],function(e,n){t[n]=!0}),t}b.Callbacks=function(e){ e="string"==typeof e?_[e]||F(e):b.extend({},e);var n,r,i,o,a,s,u=[],l=!e.once&&[],c=function(t){for(r=e.memory&&t,i=!0,a=s||0,s=0,o=u.length,n=!0;u&&o>a;a++)if(u[a].apply(t[0],t[1])===!1&&e.stopO nFalse){r=!1;break}n=!1,u&&(l?l.length&&c(l.shift()):r?u=[]:p.disable())},p={add:function(){if(u){var t=u.length;(function i(t){b.each(t,function(t,n){var r=b.type(n);"function"===r?e.unique&&p.h as(n)||u.push(n):n&&n.length&&"string"!==r&&i(n)})})(arguments),n?o=u.le ngth:r&&(s=t,c(r))}return this},remove:function(){return u&&b.each(arguments,function(e,t){var r;while((r=b.inArray(t,u,r))>-1)u.splice(r,1),n&&(o>=r&&o--,a>=r&&a--)}),

	this},has:function(e){return e?b.inArray(e,u)>-1:!(!u||!u.length)},empty: function(){return u=[],this},disable:function(){return u=l=r=t,this},disabled:function(){return!u},lock:function(){return l=t,r||p.disable(),this},locked:function(){return!l},fireWith:function(e, t){return t=t||[],t=[e,t.slice?t.slice():t],!u||i&&!l||(n?l.push(t):c(t)) ,this},fire:function(){return p.fireWith(this,arguments),this},fired:f un ction(){return!!i}};return p},b.extend({Deferred:function(e){var t=[["resolve","done",b.Callbacks("once memory"),"resolved"],["reject","fail",b.Callbacks("once memory"),"rejected"],["notif

5	OPTIONS方法启用【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00126
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此Web服务器上启用了HTTP OPTIONS方法。 OPTIONS方法提供了Web服务器支持的方法列表，它表示对有关由Request-URI标识的请求/响应链上可用的通信选项的信息的请求。
风险影响	OPTIONS方法可能会公开敏感信息，这些信息可能有助于恶意用户准备更高级的攻击。
解决方案	建议在Web服务器上禁用OPTIONS方法。
风险举证	举证描述： - 页面：http://th-info.com 请求： OPTIONS HTTP/1.1 Host: th-info.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive Content-Length: 0 响应： HTTP/1.1 200 OK Allow: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/7.5 Public: OPTIONS, TRACE, GET, HEAD, POST Date: Wed, 19 Feb 2025 10:00:21 GMT Connection: keep-alive Content-Length: 0

5.3.3 弱口令

该资产不存在弱口令风险。

5.3.3 登录入口

该资产不存在登录入口风险。

5.4 http://byw3133480001.my3w.com

5.4.1 系统漏洞

1	IIS FastCGI请求头远程溢出漏洞(CVE-2010-2730)
风险等级	高
深信服漏洞编号	SF-0005-17607
CVE编号	CVE-2010-2730
CNNVD编号	CNNVD-201009-133
CNVD编号	CNVD-2010-2000
Bugtraq编号	43138
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。对于启用了FastCGI功能的IIS服务器，远程攻击者可以通过提交特制的HTTP请求触发缓冲区溢出，导致执行任意代码。
风险影响	影响IIS:7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS10-065）以及相应补丁 MS10-065：Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-065
风险举证	IIS:7.5

2	IIS FTPSVC远程拒绝服务漏洞(CVE-2010-3972)
风险等级	高
深信服漏洞编号	SF-0005-17606
CVE编号	CVE-2010-3972
CNNVD编号	CNNVD-201012-307
CNVD编号	
Bugtraq编号	45542
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。Windows 7 IIS 7.5处理请求中的Telnet协议转义时存在的堆溢出问题，远程可以利用此漏洞导致服务器程序崩溃，拒绝服务合法用户或导致执行任意代码。
风险影响	影响IIS:7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS11-004）以及相应补丁 MS11-004：Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011

	/ms11-004
风险举证	IIS:7.5

3	IIS 重复参数请求拒绝服务漏洞(CVE-2010-1899)
风险等级	中
深信服漏洞编号	SF-0005-17608
CVE编号	CVE-2010-1899
CNNVD编号	CNNVD-201009-126
CNVD编号	CNVD-2010-1985
Bugtraq编号	43140
风险端口	80
风险描述	Microsoft Internet信息服务（IIS）是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。IIS中的脚本处理代码在处理重复的参数请求时存在栈溢出漏洞，远程攻击者可以通过对IIS所承载网站的ASP页面发送特制URI请求来利用这个漏洞，导致服务崩溃。
风险影响	影响IIS:6.0版本,7.5版本
解决方案	Microsoft已经为此发布了一个安全公告（MS10-065）以及相应补丁 MS10-065：Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960) 链接：https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-065
风险举证	IIS:7.5

5.4.2 web漏洞

1	Javascript库不安全【原理扫描】
风险等级	中
深信服漏洞编号	SF-0000-0382
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	正在使用易受攻击的Javascript库。 已报告此版本的Javascript库存在一个或多个漏洞。 有关受影响的库和所报告的漏洞的更多信息，请查阅攻击详细信息和Web参考。
风险影响	有关更多信息，请参考Web参考。
解决方案	升级到最新版本。

风险举证	举证描述： Detected Javascript library jquery version 1.4.1. The version was detected from name. 页面：http://byw3133480001.my3w.com/statics/jquery-1.4.1.js 请求： GET /statics/jquery-1.4.1.js HTTP/1.1 Cookie : ASPSESSIONIDAABABCCC=CHAMIHMCDECGAJLOCLJFNMFJ;JSESSIONID=84966XC1-SCGN358NEBOI26OZUV263-B2KAVB7M-468K9;tmp0=eNpFy7kKwjAAAFAQHHXzBzqnIUeba8uFhrZpMVprHUTq4uDmIIj%2FbjfXB2%2B32evo2qbXdXD64G3rfOXPyxhO3bBKPqXQxmsza40un8ddZaKQjAOW58Iuly1F9AYFwtB47AmjuSGV7g1v8oKJSmZgeinMqZwP5yUqJbhNf%2BBIUPB8K%2FRdhG6NSQGxpFAKiAUdf27GJvE%3D Referer : http://byw3133480001.my3w.com/statics/jquery-1.4.1.js User-Agent : Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 响应： HTTP/1.1 200 OK Content-Type : text/html Content-Encoding : gzip Last-Modified : Mon, 14 Aug 2017 06:26:53 GMT Accept-Ranges : bytes ETag : "49f7aa51c614d31:0" Vary : Accept-Encoding Server : Microsoft-IIS/7.5 Date : Wed, 19 Feb 2025 12:07:12 GMT Content-Length : 1411<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title>\xe5\x8c\x97\xe4\xba\xac\xe5\x90\x8c\xe6\x96\xb9\xe5\x85\x89\xe7\x9b\x98\xe8\x82\xa1\xe4\xbb\xbd\xe6\x9c\x89\xe9\x99\x90\xe5\x85\xac\xe5\x8f\xb8</title> <meta name="keywords" content="\xe5\x90\x8c\xe6\x96\xb9\xe5\x85\x89\xe7\x9b\x98,\xe5\x8c\x97\xe4\xba\xac\xe5\x90\x8c\xe6\x96\xb9\xe5\x85\x89\xe7\x9b\x98\xe8\x82\xa1\xe4\xbb\xbd\xe6\x9c\x89\xe9\x99\x90\xe5\x85\xac\xe5\x8f\xb8"> <meta name="description" content="\xe5\x8c\x97\xe4\xba\xac\xe5\x90\x8c\xe6\x96\xb9\xe5\x85\x89\xe7\x9b\x98\xe8\x82\xa1\xe4\xbb\xbd\xe6\x9c\x89\xe9\x99\x90\xe5\x85\xac\xe5\x8f\xb8\xe4\xbd\x9c\xe4\xb8\xba\xe5\x90\x8c\xe6\x96\xb9\xe8\x82\xa1\xe4\xbb\xbd\xe6\x9c\x89\xe9\x99\x90\xe5\x85\xac\xe5\x8f\xb8\xe5\x85\xa8\xe8\xb5\x84\xe5\xad\x90\xe5\x85\xac\xe5\x8f\xb8\xef\xbc\x8c\xe6\xb3\xa8\xe5\x86\x8c\xe8\xb5\x84\xe6\x9c\xac4000\xe4\xb8\x87\xef\xbc\x8c\xe6\x98\xaf\xe6\x9c\x80\xe6\x97\xa9\xe4\xbb\x8e\xe4\xba\x8b\xe5\x85\x89\xe5\xad\x98\xe5\x82\xa8\xe5\xae\x89\xe5\x85\xa8\xe4\xb8\x8e\xe5\xba\x94\xe7\x94\xa8\xe7\x9a\x84\xe9\xab\x98\xe6\x96\xb0\xe6\x8a\x80\xe6\x9c\xaf\xe4\xbc\x81\xe4\xb8\x9a\xe4\xb9\x8b\xe4\xb8\x80\xef\xbc\x8c\xe5\x85\xac\xe5\x8f\xb8\xe5\x88\x9b\xe7\xab\x8b\xe4\xba\x86\xe5\x9b\xbd\xe5\x86\x85\xe7\xac\xac\xe4\xb8\x80\xe5\xae\xb6\xe5\x85\x89\xe7\x9b\x98\xe8\x87\xaa\xe6\x9c\x89\xe5\x93\x81\xe7\x89\x8c\xef\xbc\x8c\xe6\x98\xaf\xe7\xa7\xbb\xe5\x8a\xa8\xe5\xad\x98\xe5\x82\xa8\xe9\xa2\x86\xe5\x9f\x9f\xe7\x9a\x84\xe4\xb8\x93\xe4\xb8\x9a\xe5\x88\xb6\xe9\x80\xa0\xe5\x95\x86\xe5\x92\x8c\xe5\x85\x89\xe7\x9b\x98\xe5\xae\x89\xe5\x85\xa8\xe5\xad\x98\xe5\x82\xa8\xe5\x8f\x8a\xe6\x81\xa2\xe5\xa4\x8d\xe7\x9a\x84\xe4\xb8\x93\xe4\xb8\x9a\xe6\x9c\x8d\xe5\x8a\xa1\xe5\x95\x86\xe3\x80\x82"> <link href="css/404.css" rel="stylesheet" type="text/css" /> <!--[if lte IE 8]> <style type="text/css"> h2 em{color:#e4ebf8;} </style> <![endif]--> </head> <body> <h1> </h1> <h2>404 Error: \xe6\x8a\xb1\xe6\xad\x89, \xe6\x82\xa8\xe6\x89\x80\xe6\x9f\xa5\xe6\x89\xbe\xe7\x9a\x84\xe9\xa1\xb5\xe9\x9d\xa2\xe4\xb8\x8d\xe5\xad\x98\xe5\x9c\xa8, \xe5\x8f\xaf\xe8\x83\xbd\xe5\xb7\xb2\xe8\xa2\xab\xe5\x88\
	xa0\xe9\x99\xa4\xe6\x88\x96\xe6\x82\xa8\xe8\xbe\x93\xe9\x94\x99\xe4\xba\x86\xe7\xbd\x91\xe5\x9d\x80!</h2> <p class="link"> ◂\xe8\xbf\x94\xe5\x9b\x9e\xe9\xa6\x96\xe9\xa1\xb5 ◂\xe8\xbf\x94\xe5\x9b\x9

风险举证	e\xe4\xb8\x8a\xe4\xb8\x80\xe9\xa1\xb5 <dl class="texts"> <dt>\xe6\xb2\xa1\xe6\x9c\x89\xe5\x8f\x91\xe7\x8e\xb0\xe4\xbd\xa0\xe8\xa6 \x81\xe6\x89\xbe\xe7\x9a\x84\xe9\xa1\xb5\xe9\x9d\xa2, \xe7\xbb\x8f\xe7\xa0\x96\xe5\xae\xb6\xe4\xbb\x94\xe7\xbb\x86\xe7\xa0\x94 \xe7\xa9\xb6\xe7\xbb\x93\xe6\x9e\x9c\xe5\xa6\x82\xe4\xb8\x8b:</dt> <dd> \xe8\xb4\xb5\xe7\x8e\x89\xe6\x89\x8b\xe8\xbe\x93\xe5\x85\x a5\xe 5\x9c\xb0\xe5\x9d\x80\xe6\x97\xb6\xe5\x8f\xaf\xe8\x83\xbd\xe5\xad\ x98\xe 5\x9c\xa8\xe9\x94\xae\xe5\x85\xa5\xe9\x94\x99\xe8\xaf\xaf \xe7\xbb\xb4\xe4\xbf\xae\xe6\x97\xb6\xe4\xb8\x8d\xe5\xb0\x8f\xe5\xbf \x83\xe6\x8a\x8a\xe9\xa1\xb5\xe9\x9d\xa2\xe6\x92\x95\xe6\x8e\x89\xe4\xb a \x86 \xe7\x94\xb5\xe4\xbf\xa1\xe7\xbd\x91\xe9\x80\x9a\xe9\x82 \x a3\xe5\xa4\xb4\xe6\x8e\xa5\xe5\x8f\xa3\xe7\x94\x9f\xe9\x94\x88\xe4\xb a\x 86 </dd> </dl> </body> </html>

2	OPTIONS方法启用【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00126
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此Web服务器上启用了HTTP OPTIONS方法。 OPTIONS方法提供了Web服务器支持的方法列表，它表示对有关由Request-URI标识的请求/响应链上可用的通信选项的信息的请求。
风险影响	OPTIONS方法可能会公开敏感信息，这些信息可能有助于恶意用户准备更高级的攻击。
解决方案	建议在Web服务器上禁用OPTIONS方法。
风险举证	举证描述： - 页面：http://byw3133480001.my3w.com 请求： OPTIONS HTTP/1.1 Host: byw3133480001.my3w.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive Content-Length: 0 响应： HTTP/1.1 200 OK Allow: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/7.5 Public: OPTIONS, TRACE, GET, HEAD, POST Date: Wed, 19 Feb 2025 10:00:17 GMT Connection: keep-alive Content-Length: 0

3	Microsoft IIS版本泄露【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00136
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	

风险端口	80
风险描述	此web应用程序返回的HTTP响应包括名为Server的头。此头的值包括Microsoft IIS服务器的版本。
风险影响	HTTP头可能会泄漏敏感信息。这些信息可以进行发动进一步的攻击。
解决方案	Microsoft IIS应该配置为从响应中删除不需要的HTTP响应标头。 有关更多信息，请参考网络参考。
风险举证	举证描述： - 页面：http://byw3133480001.my3w.com 请求： GET HTTP/1.1 Host: byw3133480001.my3w.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 404 Not Found Cache-Control: private Content-Length: 2320 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDACCDDDDD=GKDMNJMCGKOPEEAFDFKCHHIC; path=/ Date: Wed, 19 Feb 2025 10:00:19 GMT Connection: keep-alive <!DOCTYPE html PUBLIC " -//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 网站访问报错</title> <style type="text/css"> * { padding:0; margin:0;} li { list-style:none;} img { border:none;} .clear { zoom:1;} . clear:after { content:'\20'; clear:both; display:block;}

5.4.3 弱口令

该资产不存在弱口令风险。

5.4.3 登录入口

该资产不存在登录入口风险。

5.5 http://www.th-info.com

5.5.1 系统漏洞

该资产不存在系统漏洞风险。

5.5.1 web漏洞

1	ASP.NET版本泄露【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00137

CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此Web应用程序返回的HTTP响应包括名为 X-AspNet-Version 的标头。 Visual Studio使用此标头的值来确定正在使用哪个版本的ASP.NET。 对于生产站点而言，这不是必需的，应该禁用。
风险影响	HTTP标头可能会泄露敏感信息。 此信息可用于发起进一步的攻击。
解决方案	对web.config文件应用以下更改以防止ASP.NET版本泄漏：<System.Web> <httpRuntime enable VersionHeader="false" /> </System.Web>
风险举证	举证描述： - 页面：http://www.th-info.com 请求： GET /|~.aspx HTTP/1.1 Host: www.th-info.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 500 Internal Server Error Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/7.5 X-AspNet-Version: 2.0.50727 Date: Wed, 19 Feb 2025 10:00:12 GMT Connection: keep-alive Content-Length: 2907 <html> <head> <title>运行时错误</title> <style> body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;} p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px} b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px} H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red } H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon } pre {font-family:"Lucida Console";font-size: .9em} .marker {font-weight: bold; color: black;text-decoration: none;} .version {color: gray;} .error {margin-bottom: 10px;} .expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:hand; } </style> </head>

2	cookie 没有设置httponly标志位【原理扫描】
风险等级	低
深信服漏洞编号	SF-2021-00870
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	HttpOnly 主要是为了限制web页面程序的browser端script程序读取cookie，防止恶意代码获取客户的敏感信息。
风险影响	远程攻击者可以利用此漏洞获取敏感信息
解决方案	为SetCookie配置HttpOnly属性
	举证描述： - 页面：http://www.th-info.com 请求： GET HTTP/1.1 Host: www.th-info.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 404

风险举证	Not Found Cache-Control: private Content-Length: 2320 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDACCDDDDD=IMCMNJMCBHHAFGNDBIIPMMBE; path=/ Date: Wed, 19 Feb 2025 10:00:15 GMT Connection: keep-alive <!DOCTYPE html PUBLIC " -//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 网站访问报错</title> <style type="text/css"> * { padding:0; margin:0;} li { list-style:none;} img { border:none;} .clear { zoom:1;} . clear:after { content:'\20'; clear:both; display:block;}

3	general 未设置cookie的Secure标志位【原理扫描】
风险等级	低
深信服漏洞编号	SF-2016-00025
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	通用型(general)漏洞并不针对某一系统，其在各类系统中都有可能存在。Cookie Without Secure Flag Set是指服务器Set-Cookie消息头中未设置可选属性Secure，如果服务器设置这个属性，那么cookie只能在HTTPS请求中提交。
风险影响	影响所有Set-Cookie消息头中未设置可选属性Secure的系统
解决方案	为cookie设置Secure属性
风险举证	举证描述： - 页面：http://www.th-info.com 请求： GET HTTP/1.1 Host: www.th-info.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 404 Not Found Cache-Control: private Content-Length: 2320 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDACCDDDDD=IMCMNJMCBHHAFGNDBIIPMMBE; path=/ Date: Wed, 19 Feb 2025 10:00:15 GMT Connection: keep-alive <!DOCTYPE html PUBLIC " -//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 网站访问报错</title> <style type="text/css"> * { padding:0; margin:0;} li { list-style:none;} img { border:none;} .clear { zoom:1;} . clear:after { content:'\20'; clear:both; display:block;}

4	OPTIONS方法启用【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00126
CVE编号	-
CNNVD编号	

CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此Web服务器上启用了HTTP OPTIONS方法。 OPTIONS方法提供了Web服务器支持的方法列表，它表示对有关由Request-URI标识的请求/响应链上可用的通信选项的信息的请求。
风险影响	OPTIONS方法可能会公开敏感信息，这些信息可能有助于恶意用户准备更高级的攻击。
解决方案	建议在Web服务器上禁用OPTIONS方法。
风险举证	举证描述： - 页面：http://www.th-info.com 请求： OPTIONS HTTP/1.1 Host: www.th-info.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive Content-Length: 0 响应： HTTP/1.1 200 OK Allow: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/7.5 Public: OPTIONS, TRACE, GET, HEAD, POST Date: Wed, 19 Feb 2025 10:00:11 GMT Connection: keep-alive Content-Length: 0

5	Microsoft IIS版本泄露【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00136
CVE编号	-
CNNVD编号	
CNVD编号	
Bugtraq编号	
风险端口	80
风险描述	此web应用程序返回的HTTP响应包括名为Server的头。此头的值包括Microsoft IIS服务器的版本。
风险影响	HTTP头可能会泄漏敏感信息。这些信息可以进行发动进一步的攻击。
解决方案	Microsoft IIS应该配置为从响应中删除不需要的HTTP响应标头。 有关更多信息，请参考网络参考。
风险举证	举证描述： - 页面：http://www.th-info.com 请求： GET HTTP/1.1 Host: www.th-info.com:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 404 Not Found Cache-Control: private Content-Length: 2320 Content-Type: text/html Server: Microsoft-IIS/7.5 Set-Cookie: ASPSESSIONIDACCDDDDD=CPBMNJMCLDECIJNNFBODCKMI; path=/ Date: Wed, 19 Feb 2025 10:00:11 GMT Connection: keep-alive <!DOCTYPE html PUBLIC " -//W3C//DTD XHTML 1.0 Transitional//EN" " http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title> 网站访问报错</title> <style type="text/css"> * { padding:0; margin:0;} li { list-style:none;} img { border:none;} .clear { zoom:1;} .clear:after { content:'\20'; clear:both; display:block;}

5.5.2 弱口令

该资产不存在弱口令风险。

5.5.2 登录入口

该资产不存在登录入口风险。

6 参考标准

6.1 单一系统漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
严重	9 <= 漏洞风险值 <= 10	漏洞可能导致系统崩溃、数据泄露等严重后果，易受攻击，影响范围广，修复难度大，需要立即修复。
高危	7 <= 漏洞风险值 < 9	漏洞可能导致系统受到攻击或数据被盗取，易受攻击，影响范围较广，修复难度较大，需要尽快修复。
中危	4 <= 漏洞风险值 < 7	漏洞可能导致系统受到攻击或数据泄露，易受攻击，影响范围较小，修复难度一般，需要在合理的时间内修复。
低危	0 <= 漏洞风险值 < 4	漏洞可能导致系统受到攻击或数据泄露的风险较小，不易受攻击，修复难度较小，可以在合理的时间内修复。

6.2 单一web漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
严重	9 <= 漏洞风险值 <= 10	漏洞可能导致系统崩溃、数据泄露等严重后果，易受攻击，影响范围广，修复难度大，需要立即修复。
高危	7 <= 漏洞风险值 < 9	漏洞可能导致系统受到攻击或数据被盗取，易受攻击，影响范围较广，修复难度较大，需要尽快修复。
中危	4 <= 漏洞风险值 < 7	漏洞可能导致系统受到攻击或数据泄露，易受攻击，影响范围较小，修复难度一般，需要在合理的时间内修复。
低危	0 <= 漏洞风险值 < 4	漏洞可能导致系统受到攻击或数据泄露的风险较小，不易受攻击，修复难度较小，可以在合理的时间内修复。

6.3 单一资产风险等级评定标准

危险程度	危险程度说明
高危	资产存在高危风险的漏洞，风险等级为高风险，建议优先关注。
中危	资产只发现中危及以下风险等级的漏洞，风险等级为中风险。
低危	资产只发现低危风险的漏洞，风险值等级较低。
安全	不存在高中低风险的漏洞，不存在脆弱性风险。

6.4 安全建议

2017年6月1日起《中华人民共和国网络安全法》（下文简称《网络安全法》）正式实施。这意味着网络运营者（指网络的所有者、管理者和网络服务提供者）必须担负起履行网络安全的法律责任。

随着网络安全技术的不断发展，道高一尺魔高一丈，网络安全的本质就是人与人的对抗和博弈，没有百分之百的安全，也没有百分之百的成功入侵，但网络安全的门槛永远是可以不断提高的。外网安全防护只是网络运营企业网络安全的第一道防线，真正的对抗仍然是发生在具有核心业务系统及核心业务数据的内网，内网才是真正的主战场。近几年，各大网络安全事件无不印证此观点，无论是国内CSDN、163、12306等用户个人信息泄漏事件，还是境外针对全球特定目标的APT攻击，如：“丰收行动”、摩诃草事件、震网病毒事件等，都是突破外网安全防护的第一道防线，长期潜伏于内网而未被及时检测和发现导致的。

因此，外网安全防护是网络安全的第一道防线，真正的网络安全主战场仍然是内网网络安全。针对内网安全，我们建议采用如下措施来降低内网安全风险：

- 内网业务系统在设计阶段，需要考虑安全机制、安全设备和安全管理等因素
- 内网安全域划分，对内网不同业务系统，按照安全风险等级要求进行安全域划分
- 请专业人员定期对内网进行渗透测试，发现安全漏洞，及时修复
- 请专业人员定期对内网弱口令进行排查，加强弱口令安全管理，对业务系统密码复杂度进行要求，如：长度至少8位，包含字母、数字、特殊字符等
- 对内部人员进行安全意识培训，通过管理手段和安全意识培训降低内网安全风险事件的发生
- 对关键业务系统进行定期备份