漏洞扫描安全评估报告

1 检测结果综述

本次报告中，主机【10.129.57.55】共检测出风险8个，其中系统漏洞8个，Web漏洞0个，弱口令0个。

整体风险值为7.3，安全等级为 比较危险 。所有漏洞中，高危漏洞0个，中危漏洞4个，低危漏洞1个，信息级漏洞3个。（漏洞风险等级的分类规则及资产风险等级分类规则，请参见章节《资产风险等级评定标准》）。

2 资产总体概览

2.1 资产基本信息

系统资产列表：

主机名称	10.129.57.55
主机资产	10.129.57.55
操作系统	
MAC地址	
扫描时间	系统扫描： 开始时间：2025-05-04 17:36:06 至 2025-05-04 17:55:39 (耗时：19分33秒)
资产风险值	7.3
漏洞分布	漏洞总计：8 高风险：0 中风险：4 低风险：1 信息风险：3
漏洞状态标识	新增：8 误报：0 已修复：0
资产组	湘潭市生态环境局-重点污染源自动监控与基础数据库系统、默认资产组
标签	
系统版本	V3.0(6.8.0-R1-v91413-20230824)
规则库版本	20250331171220

WEB资产列表：

2.2 整体漏洞统计

本报告中包含【1】个主机资产，该主机中存在【0】个Web站点，对主机和Web进行整体漏洞分析的情况如下表所示。主机和Web详细漏洞信息见章节4，章节5。

IP/URL	高	中	低	信息	总计
系统漏洞	0	4	1	3	8
WEB漏洞	0	0	0	0	0
总计	**0**	**4**	**1**	**3**	**8**

2.3 敏感端口/服务

本次任务检测到开放了以下【1】种敏感端口或服务，具体情况如下表所示:

序号	端口	服务	协议
1	18080	http	TCP

说明：敏感端口/服务指根据安全研究表明，容易被黑客利用漏洞发起攻击的端口/服务。

2.4 敏感中间件

本次任务检测到以下【0】种敏感中间件，具体情况如下表所示:

序号	中间件

说明：敏感中间件是指安全研究表明，容易被黑客利用发起攻击的中间件。

3 资产端口服务信息

资产的端口/服务开放情况如下表所示，共开放了【1】个端口:

端口	服务	协议	漏洞总数
18080	http	TCP	6

漏洞名称	cve编号	信息
jQuery 跨站脚本漏洞 (CVE-2020-11023)	CVE-2020-11023	jquery:jquery 1.12.4 >= 1.0.3 and jquery:jquery 1.12.4 < 3.5.0
jQuery 跨站脚本漏洞 (CVE-2015-9251)	CVE-2015-9251	jquery:jquery 1.12.4 < 3.0.0
jQuery 跨站脚本漏洞 (CVE-2019-11358)	CVE-2019-11358	jquery:jquery 1.12.4 < 3.4.0
jQuery 跨站脚本漏洞 (CVE-2020-11022)	CVE-2020-11022	jquery:jquery 1.12.4 >= 1.2 and jquery:jquery 1.12.4 < 3.5.0
远程主机Web服务404检查【原理扫描】		远程主机Web服务404检查
探测到jquery		jquery version: 1.12.4 detected from /static/component/jquery-1.12.4.js

--	--	TCP	1

漏洞名称	cve编号	信息
允许Traceroute探测		Here is the route from 10.129.32.98 to 10.129.57.55: 10.129.32.98 ?

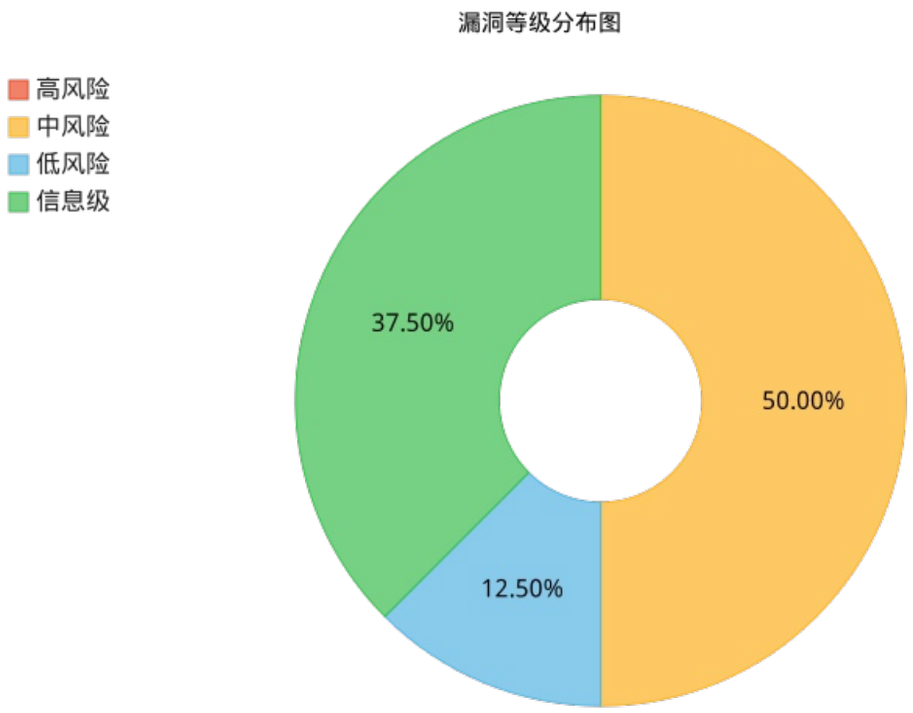
--	--	ICMP	1

漏洞名称	cve编号	信息
ICMP时间戳检测	CVE-1999-0524	--

4 主机漏洞信息

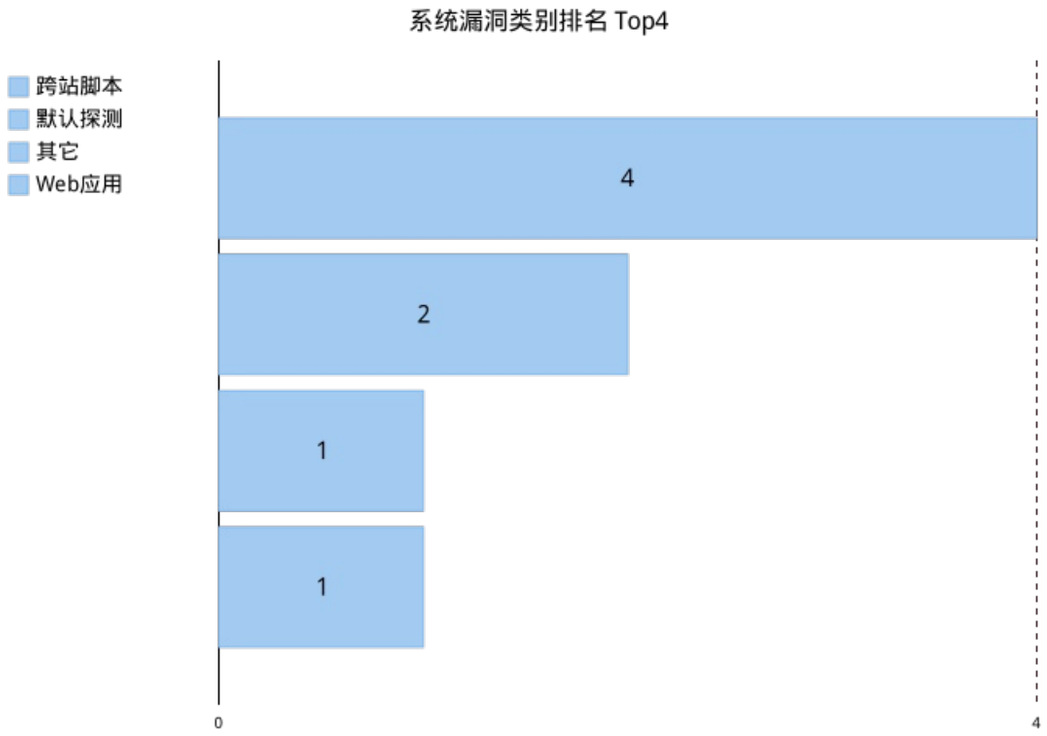
4.1 主机漏洞统计概况

4.1.1 漏洞等级分布



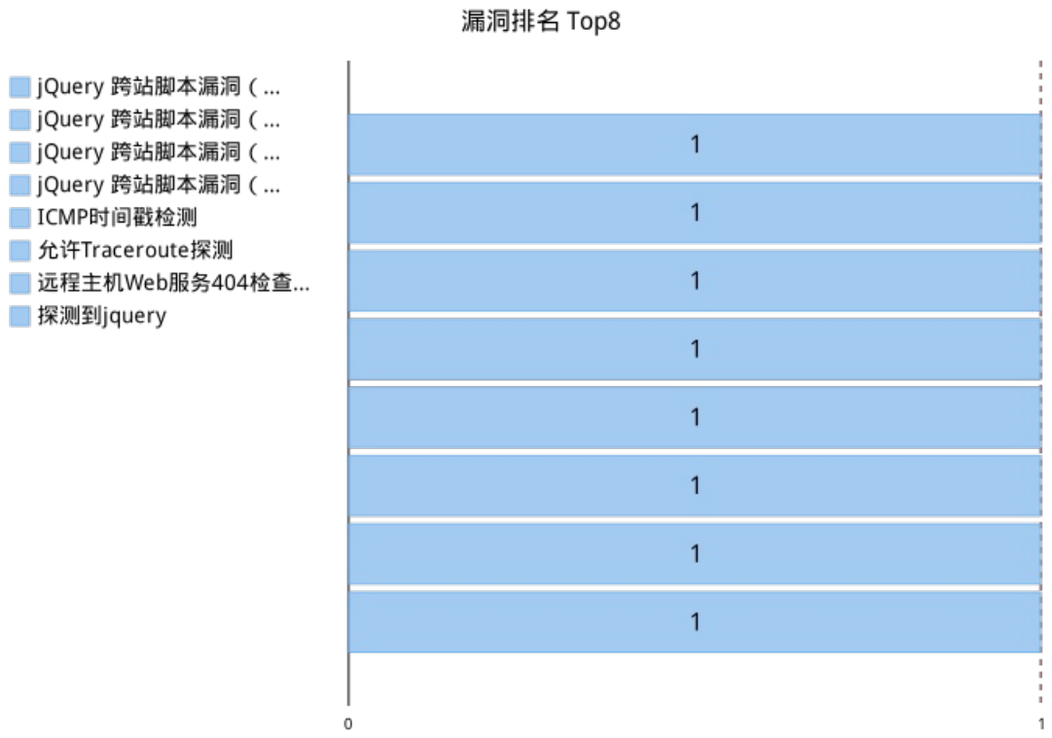
高风险	中风险	低风险	信息级	总计
0	4	1	3	8

4.1.2 漏洞类别统计



序号	主机漏洞类别（TOP10）	总计
1	跨站脚本	4
2	默认探测	2
3	其它	1
4	Web应用	1

4.1.3 漏洞排名



序号	系统漏洞名称（TOP10）	总计
1	jQuery 跨站脚本漏洞（CVE-2015-9251）	1
2	jQuery 跨站脚本漏洞（CVE-2019-11358）	1
3	jQuery 跨站脚本漏洞（CVE-2020-11023）	1
4	jQuery 跨站脚本漏洞（CVE-2020-11022）	1
5	ICMP时间戳检测	1
6	允许Traceroute探测	1
7	远程主机Web服务404检查【原理扫描】	1
8	探测到jquery	1

4.2 主机漏洞详情

漏洞名称	漏洞分类	漏洞类型	出现次数
⊟ jQuery 跨站脚本漏洞（CVE-2015-9251）	跨站脚本	中风险	1

漏洞编号	1104897
风险级别	中风险
概要	

描述	jQuery是美国John Resig个人开发者的一套开源、跨浏览器的JavaScript库。该库简化了HTML与JavaScript之间的操作，并具有模块化、插件扩展等特点。 jQuery 3.0.0之前版本中存在跨站脚本漏洞。该漏洞源于WEB应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。
解决办法	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： https://jquery.com/
详情请参阅	https://www.securityfocus.com/bid/105658 https://access.redhat.com/errata/RHSA-2020:0729 https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html https://ics-cert.us-cert.gov/advisories/ICSA-18-212-04 https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin_LFSec126.pdf https://jquery.org/ https://github.com/jquery/jquery/pull/2588 https://github.com/jquery/jquery/commit/f60729f3903d17917dc351f3ac87794de379b0cc http://www.securityfocus.com/bid/105658 https://www.oracle.com/security-alerts/cpuapr2020.html https://security.netapp.com/advisory/ntap-20210108-0004/ https://github.com/jquery/jquery/issues/2432 https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html https://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html https://seclists.org/bugtraq/2019/May/18 https://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html https://github.com/jquery/jquery/pull/2588/commits/c254d308a7d3f1eac4d0b42837804cfffcba4bb2 http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html https://www.oracle.com/security-alerts/cpuoct2020.html http://packetstormsecurity.com/files/153237/RetireJS-CORS-Issue-Script-Execution.html https://access.redhat.com/errata/RHSA-2020:0481 http://seclists.org/fulldisclosure/2019/May/11 http://seclists.org/fulldisclosure/2019/May/10 https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E http://seclists.org/fulldisclosure/2019/May/13 https://packetstormsecurity.com/files/153237/RetireJS-CORS-Issue-Script-Execution.html https://www.oracle.com/security-alerts/cpujan2020.html https://lists.apache.org/thread.html/54df3aeb4239b64b50b356f0ca6f986e3c4ca5b84c515dce077c7854@%3Cuser.flink.apache.org%3E https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44601 http://lists.opensuse.org/opensuse-security-announce/2020-03/msg00041.html https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E https://snyk.io/vuln/npm:jquery:20150627 https://lists.apache.org/thread.html/17ff53f7999e74fbe3cc0ceb4e1c3b00b180b7c5afec8e978837bc49@%3Cuser.flink.apache.o

rg%3E
https://lists.apache.org/thread.html/10f0f3aefd51444d1198c65f44ffdf2d78ca3359423dbc1c168c9731@%3Cdev.flink.apache.org%3E
https://www.tenable.com/security/tns-2019-08
http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
https://lists.apache.org/thread.html/52bafac05ad174000ea465fe275fd3cc7bd5c25535a7631c0bc9bfb2@%3Cuser.flink.apache.org%3E
https://lists.apache.org/thread.html/ba79cf1658741e9f146e4c59b50aee56656ea95d841d358d006c18b6@%3Ccommits.roller.apache.org%3E
https://www.oracle.com/security-alerts/cpujul2020.html
https://www.ibm.com/support/pages/node/1105515
https://www.ibm.com/support/pages/node/1105509
https://www.ibm.com/support/pages/node/1105479
https://www.ibm.com/support/pages/node/1106577
https://access.redhat.com/errata/RHSA-2020:0481
http://www.ibm.com/support/docview.wss?uid=ibm10874666
https://fortiguard.com/psirt/FG-IR-18-013
https://www.ibm.com/support/docview.wss?uid=ibm10967469
https://www.oracle.com/security-alerts/cpujul2020.html
https://www.ibm.com/blogs/psirt/security-bulletin-a-cross-site-scripting-vulnerability-in-jquery-affects-ibm-infosphere-information-server/
https://packetstormsecurity.com/files/159353/Red-Hat-Security-Advisory-2020-3936-01.html
https://www-01.ibm.com/support/docview.wss?uid=ibm10878200
https://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
https://www.ibm.com/blogs/psirt/security-bulletin-multiple-security-vulnerabilities-in-swagger-ui-affect-ibm-business-automation-workflow-and-ibm-business-process-manager-bpm/
https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilites-affect-ibm-jazz-foundation-and-ibm-engineering-products-5/
https://www.auscert.org.au/bulletins/ESB-2019.4294/
https://www.ibm.com/blogs/psirt/security-bulletin-cross-site-scripting-and-vulnerable-library-jquery-v1-11-1-affects-ibm-engineering-workflow-management/
https://www.ibm.com/blogs/psirt/security-bulletin-multiple-security-vulnerabilities-in-swagger-ui-affect-ibm-business-automation-workflow-and-ibm-business-process-manager-bpm-2/
https://www.auscert.org.au/bulletins/ESB-2021.0465
https://packetstormsecurity.com/files/156630/Red-Hat-Security-Advisory-2020-0729-01.html
https://www.auscert.org.au/bulletins/78866
https://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html
https://packetstormsecurity.com/files/156941/Red-Hat-Security-Advisory-2020-0983-01.html
https://www.ibm.com/support/pages/node/1105497
https://www.auscert.org.au/bulletins/ESB-2020.3875/
https://www.auscert.org.au/bulletins/ESB-2020.1016/
https://www.auscert.org.au/bulletins/ESB-2021.1519
https://www.auscert.org.au/bulletins/ESB-2020.3902/
https://www.auscert.org.au/bulletins/ESB-2020.0832/
https://packetstormsecurity.com/files/170821/Red-Hat-Security-Advisory-2023-0552-01.html
https://www.auscert.org.au/bulletins/ESB-2023.0585
https://packetstormsecurity.com/files/159852/Red-Hat-Security-Advisory-2020-4847-01.html

	https://www.auscert.org.au/bulletins/ESB-2021.2525 http://www-01.ibm.com/support/docview.wss?uid=ibm10874666 https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-is-vulnerable-to-using-components-with-known-vulnerabilities-10/ https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-is-vulnerable-to-using-components-with-known-vulnerabilities-8/ https://us-cert.cisa.gov/ics/advisories/icsma-21-187-01 https://www.auscert.org.au/bulletins/ESB-2023.0583 https://www.ibm.com/blogs/psirt/security-bulletin-ibm-security-qradar-analyst-workflow-add-on-to-ibm-qradar-siem-is-vulnerable-to-using-components-with-known-vulnerabilities-2/ https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerability-issues-affect-ibm-spectrum-symphony-7-3-1/ https://www.auscert.org.au/bulletins/79122 https://www.auscert.org.au/bulletins/ESB-2020.0494/ https://www.securityfocus.com/bid/105658 https://www.auscert.org.au/bulletins/78794 https://packetstormsecurity.com/files/156315/Red-Hat-Security-Advisory-2020-0481-01.html https://www.auscert.org.au/bulletins/ESB-2020.3267/ https://us-cert.cisa.gov/ics/advisories/icsa-22-097-01 https://www.auscert.org.au/bulletins/ESB-2020.1076/ https://www.auscert.org.au/bulletins/ESB-2020.3368/ https://packetstormsecurity.com/files/170823/Red-Hat-Security-Advisory-2023-0553-01.html https://www.ibm.com/blogs/psirt/security-bulletin-ibm-security-guardium-is-affected-by-multiple-vulnerabilities-3/ https://www.auscert.org.au/bulletins/ESB-2019.3165/ https://www.auscert.org.au/bulletins/ESB-2022.1512
CVE	CVE-2015-9251
CVSS	6.1
CNCVE	CNCVE-20159251
CNNVD	CNNVD-201801-798
检测详情	主机：10.129.57.55| 端口：18080| 服务：http| 协议：TCP jquery:jquery 1.12.4 < 3.0.0 漏洞状态：新增

⊟ jQuery 跨站脚本漏洞（CVE-2019-11358）	跨站脚本	中风险	1

漏洞编号	1124911
风险级别	中风险
概要	
描述	jQuery是美国John Resig个人开发者的一套开源、跨浏览器的JavaScript库。该库简化了HTML与JavaScript之间的操作，并具有模块化、插件扩展等特点。 jQuery 3.4.0之前版本中存在跨站脚本漏洞，该漏洞源于WEB应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。
解决办法	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

详情请参阅	https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/KYH3OAGR2RTCHRA5NOKX2TES7SNQMWGO/ https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html https://www.debian.org/security/2019/dsa-4434 https://www.drupal.org/sa-core-2019-006 https://backdropcms.org/security/backdrop-sa-core-2019-009 https://github.com/jquery/jquery/releases https://jquery.org/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://github.com/jquery/jquery/pull/4333 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/backdrop/backdrop/releases https://snyk.io/vuln/SNYK-JS-JQUERY-174006 https://lists.apache.org/thread.html/r38f0d1aa3c923c22977fe7376508f030f22e22c1379fbb155bf29766@%3Cdev.syncope.apache.org%3E https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/5IABSKTYZ5JUGL735UKGXL5YPRYOPUYI/ https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html https://www.oracle.com/security-alerts/cpujan2020.html https://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html https://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html https://www.oracle.com/security-alerts/cpuoct2020.html https://seclists.org/bugtraq/2019/Jun/12 http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00006.html https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/RLXRX23725JL366CNZGJZ7AQQB7LHQ6F/ https://lists.apache.org/thread.html/88fb0362fd40e5b605ea8149f63241537b8b6fb5bfa315391fc5cbb7@%3Ccommits.airflow.apache.org%3E https://www.debian.org/security/2019/dsa-4460 https://lists.apache.org/thread.html/r2041a75d3fc09dec55adfd95d598b38d22715303f65c997c054844c9@%3Cissues.flink.apache.org%3E https://www.synology.com/security/advisory/Synology_SA_19_19 https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/4UOAZIFCSZ3ENEFOR5IXX6NFAD3HV7FA/ https://lists.apache.org/thread.html/5928aa293e39d248266472210c50f176cac1535220f2486e6a7fa844@%3Ccommits.airflow.apache.org%3E https://lists.apache.org/thread.html/08720ef215ee7ab3386c05a1a90a7d1c852bf0706f176a7816bf65fc@%3Ccommits.airflow.apache.org%3E https://www.oracle.com/security-alerts/cpujan2021.html http://www.securityfocus.com/bid/108023 https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44601 https://access.redhat.com/errata/RHSA-2019:3024 https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E https://www.securityfocus.com/bid/108023 https://access.redhat.com/errata/RHBA-2019:1570

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/QV3PKZC3PQCO3273HAT76PAQZFBEO4KP/

https://access.redhat.com/errata/RHSA-2019:3023

https://www.tenable.com/security/tns-2019-08

https://www.oracle.com/security-alerts/cpuoct2021.html

https://lists.debian.org/debian-lts-announce/2019/05/msg00029.html

https://lists.apache.org/thread.html/ba79cf1658741e9f146e4c59b50aee56656ea95d841d358d006c18b6@%3Ccommits.roller.apache.org%3E

https://lists.apache.org/thread.html/r2baacab6e0acb5a2092eb46ae04fd6c3e8277b4fd79b1ffb7f3254fa@%3Cissues.flink.apache.org%3E

https://supportportal.juniper.net/s/article/2021-07-Security-Bulletin-Junos-OS-Multiple-J-Web-vulnerabilities-resolved-in-Junos-OS-21-2R1

https://www.oracle.com/security-alerts/cpujan2022.html

https://www.oracle.com/security-alerts/cpuapr2020.html

https://lists.debian.org/debian-lts-announce/2019/05/msg00006.html

https://lists.apache.org/thread.html/r7e8ebccb7c022e41295f6fdb7b971209b83702339f872ddd8cf8bf73@%3Cissues.flink.apache.org%3E

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WZW27UCJ5CYFL4KFFFMYMIBNMIU2ALG5/

https://seclists.org/bugtraq/2019/May/18

https://seclists.org/bugtraq/2019/Apr/32

http://packetstormsecurity.com/files/153237/RetireJS-CORS-Issue-Script-Execution.html

https://access.redhat.com/errata/RHSA-2019:2587

http://seclists.org/fulldisclosure/2019/May/11

https://lists.apache.org/thread.html/bcce5a9c532b386c68dab2f6b3ce8b0cc9b950ec551766e76391caa3@%3Ccommits.nifi.apache.org%3E

http://seclists.org/fulldisclosure/2019/May/10

https://security.netapp.com/advisory/ntap-20190919-0001/

https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

http://seclists.org/fulldisclosure/2019/May/13

https://packetstormsecurity.com/files/153237/RetireJS-CORS-Issue-Script-Execution.html

https://www.oracle.com/security-alerts/cpuApr2021.html

http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00025.html

https://lists.apache.org/thread.html/6097cdbd6f0a337bedd9bb5cc441b2d525ff002a96531de367e4259f@%3Ccommits.airflow.apache.org%3E

https://www.privacy-wise.com/mitigating-cve-2019-11358-in-old-versions-of-jquery/

https://access.redhat.com/errata/RHSA-2019:1456

https://lists.apache.org/thread.html/b736d0784cf02f5a30fbb4c5902762a15ad6d47e17e2c5a17b7d6205@%3Ccommits.airflow.apache.org%3E

https://lists.apache.org/thread.html/rca37935d661f4689cb4119f1b3b224413b22be161b678e6e6ce0c69b@%3Ccommits.nifi.apache.org%3E

https://lists.apache.org/thread.html/r7aac081cbddb6baa24b75e74abf0929bf309b176755a53e3ed810355@%3Cdev.flink.apache.org%3E

https://lists.apache.org/thread.html/r41b5bfe009c845f67d4f68948cc9419ac2d62e287804aafd72892b08@%3Cissues.flink.apac

he.org%3E

https://www.tenable.com/security/tns-2020-02

https://lists.apache.org/thread.html/rac25da84ecdcd36f6de5ad0d255f4e967209bbbebddb285e231da37d@%3Cissues.flink.apache.org%3E

https://www.oracle.com//security-alerts/cpujul2021.html

http://www.openwall.com/lists/oss-security/2019/06/03/2

https://lists.apache.org/thread.html/r7d64895cc4dff84d0becfc572b20c0e4bf9bfa7b10c6f5f73e783734@%3Cdev.storm.apache.org%3E

https://lists.debian.org/debian-lts-announce/2020/02/msg00024.html

https://www.oracle.com/security-alerts/cpujul2020.html

https://www.ibm.com/support/pages/node/1105515

https://www.ibm.com/support/pages/node/1105497

https://www.ibm.com/support/pages/node/1105479

https://www.ibm.com/support/pages/node/1106577

http://www.debian.org/security/2019/dsa-4434

https://lists.debian.org/debian-lts-announce/2019/05/msg00029.html

http://www.ibm.com/support/docview.wss?uid=ibm10886357

https://lists.debian.org/debian-lts-announce/2019/05/msg00006.html

https://www.auscert.org.au/bulletins/ESB-2022.5539

https://www.oracle.com/security-alerts/cpujul2020.html

https://www.oracle.com/security-alerts/cpuapr2021.html

https://www.oracle.com/security-alerts/cpuoct2021.html

https://www.oracle.com/security-alerts/cpujan2020verbose.html

https://www.cybersecurity-help.cz/vdb/SB2021072742

https://www.auscert.org.au/bulletins/ESB-2019.4294/

https://www.securityfocus.com/bid/108023

https://www.auscert.org.au/bulletins/80318

https://www.ibm.com/blogs/psirt/security-bulletin-security-vulnerabilities-have-been-identified-in-bigfix-platform-shipped-with-ibm-license-metric-tool-2/

https://www.auscert.org.au/bulletins/79458

https://www.oracle.com/security-alerts/cpujul2021.html

https://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html

https://www.auscert.org.au/bulletins/ESB-2020.1679/

https://www.auscert.org.au/bulletins/ESB-2020.3875/

https://packetstormsecurity.com/files/160567/Red-Hat-Security-Advisory-2020-5581-01.html

https://www.ibm.com/support/pages/node/6520510

https://nvd.nist.gov/vuln/detail/CVE-2019-11358

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-security-information-queue-uses-components-with-known-vulnerabilities-cve-2019-8331-cve-2019-11358/

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-is-vulnerable-to-using-components-with-known-vulnerabilities-10/

https://www.ibm.com/blogs/psirt/security-bulletin-security-vulnerabilities-in-dojo-and-jquery-might-affect-ibm-business-automation-workflow-and-ibm-business-process-manager-bpm-2/

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-security-guardium-insights-is-affected-by-a-jquery-vulnerabilitiy-cve-2019-11358/

https://www.auscert.org.au/bulletins/ESB-2020.2375/

https://www.auscert.org.au/bulletins/ESB-2020.2464/

https://www.oracle.com/security-alerts/cpuoct2020.html
https://packetstormsecurity.com/files/152580/Debian-Security-Advisory-4434-1.html
https://www.ibm.com/support/pages/node/1105509
https://packetstormsecurity.com/files/157102/Red-Hat-Security-Advisory-2020-1325-01.html
https://www.auscert.org.au/bulletins/ESB-2022.5150
https://www.ibm.com/blogs/psirt/security-bulletin-ibm-security-guardium-is-affected-by-multiple-vulnerabilities-3/
https://www.auscert.org.au/bulletins/ESB-2022.1512
https://packetstormsecurity.com/files/159353/Red-Hat-Security-Advisory-2020-3936-01.html
https://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
https://www.ibm.com/blogs/psirt/security-bulletin-multiple-security-vulnerabilities-in-swagger-ui-affect-ibm-business-automation-workflow-and-ibm-business-process-manager-bpm/
https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilites-affect-ibm-jazz-foundation-and-ibm-engineering-products-5/
https://www.auscert.org.au/bulletins/ESB-2019.1806/
https://www.auscert.org.au/bulletins/ESB-2020.0657/
https://www.auscert.org.au/bulletins/ESB-2020.4452/
https://www.ibm.com/blogs/psirt/security-bulletin-ibm-cognos-command-center-has-addressed-multiple-vulnerabilities-q12021/
https://packetstormsecurity.com/files/158406/Red-Hat-Security-Advisory-2020-2412-01.html
https://www.auscert.org.au/bulletins/ESB-2020.3700/
https://www.oracle.com/security-alerts/cpujan2021.html
https://www.auscert.org.au/bulletins/ESB-2020.3902/
https://www.auscert.org.au/bulletins/ESB-2019.2037/
https://packetstormsecurity.com/files/170821/Red-Hat-Security-Advisory-2023-0552-01.html
https://www.auscert.org.au/bulletins/ESB-2023.0585
https://packetstormsecurity.com/files/159852/Red-Hat-Security-Advisory-2020-4847-01.html
https://www.auscert.org.au/bulletins/ESB-2021.2525
https://www.us-cert.gov/ics/advisories/icsa-20-133-02
https://www.ibm.com/support/pages/node/1138456
https://www.auscert.org.au/bulletins/ESB-2023.1351
https://www.ibm.com/blogs/psirt/security-bulletin-security-vulnerabilities-in-dojo-and-jquery-might-affect-ibm-business-automation-workflow-and-ibm-business-process-manager-bpm/
https://www.auscert.org.au/bulletins/ESB-2023.0583
https://www.ibm.com/blogs/psirt/security-bulletin-vulnerability-in-jquery-affects-ibm-tririga-application-platform-cve-2019-11358/
https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerability-issues-affect-ibm-spectrum-symphony-7-3-1/
https://www.cybersecurity-help.cz/vdb/SB2021042845
https://www.cybersecurity-help.cz/vdb/SB2022012403
https://www.auscert.org.au/bulletins/ESB-2020.3267/
https://us-cert.cisa.gov/ics/advisories/icsa-22-097-01
https://www.ibm.com/blogs/psirt/security-bulletin-a-vulnerability-in-jquery-affects-the-ibm-performance-management-product-cve-2019-11358/
https://www.auscert.org.au/bulletins/ESB-2020.3368/
https://packetstormsecurity.com/files/169714/Red-Hat-Security-Advisory-2022-7343-01.html
https://packetstormsecurity.com/files/170823/Red-Hat-Security-Advisory-2023-0553-01.html
https://www.auscert.org.au/bulletins/ESB-2020.1220/
https://packetstormsecurity.com/files/159727/Red-Hat-Security-Advisory-2020-4298-01.html

CVE	CVE-2019-11358
CVSS	6.1
CNCVE	CNCVE-201911358
CNNVD	CNNVD-201904-948
检测详情	主机：10.129.57.55| 端口：18080| 服务：http| 协议：TCP jquery:jquery 1.12.4 < 3.4.0 漏洞状态：新增

jQuery 跨站脚本漏洞（CVE-2020-11023）	跨站脚本	中风险	1

漏洞编号	1144188
风险级别	中风险
概要	
描述	jQuery是美国John Resig个人开发者的一套开源、跨浏览器的JavaScript库。该库简化了HTML与JavaScript之间的操作，并具有模块化、插件扩展等特点。 jQuery 1.0.3版本至3.5.0之前版本中存在跨站脚本漏洞。该漏洞源于WEB应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。
解决办法	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://jquery.com/upgrade-guide/3.5/
详情请参阅	https://lists.apache.org/thread.html/ra406b3adfcffcb5ce8707013bdb7c35e3ffc2776a8a99022f15274c6@%3Cissues.hive.apache.org%3E https://security.gentoo.org/glsa/202007-03 https://lists.apache.org/thread.html/r4aadb98086ca72ed75391f54167522d91489a0d0ae25b12baa8fc7c5@%3Cissues.hive.apache.org%3E https://lists.apache.org/thread.html/r49ce4243b4738dd763caeb27fa8ad6afb426ae3e8c011ff00b8b1f48@%3Cissues.flink.apache.org%3E https://security.netapp.com/advisory/ntap-20200511-0006/ https://www.oracle.com/security-alerts/cpujul2022.html https://www.oracle.com/security-alerts/cpujul2022.html https://www.oracle.com/security-alerts/cpuoct2020.html https://lists.apache.org/thread.html/r55f5e066cc7301e3630ce90bbbf8d28c82212ae1f2d4871012141494@%3Cdev.felix.apache.org%3E https://lists.debian.org/debian-lts-announce/2021/03/msg00033.html https://lists.apache.org/thread.html/r0593393ca1e97b1e7e098fe69d414d6bd0a467148e9138d07e86ebbb@%3Cissues.hive.apache.org%3E https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SFP4UK4EGP4AFH2MWYJ5A5Z4I7XVFQ6B/ https://lists.apache.org/thread.html/r4dba67be3239b34861f1b9cfdf9dfb3a90272585dcce374112ed6e16@%3Cdev.felix.apache.org%3E https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/QPN2L2XVQGUA2V5HNQJWHK3APSK3VN7K/ https://lists.apache.org/thread.html/radcb2aa874a79647789f3563fcbbceaf1045a029ee8806b59812a8ea@%3Cissues.hive.apache.org%3E https://lists.apache.org/thread.html/rb25c3bc7418ae75cba07988dafe1b6912f76a9dd7d94757878320d61@%3Cgitbox.hive.apa

che.org%3E
https://lists.apache.org/thread.html/r07ab379471fb15644bf7a92e4a98cbc7df3cf4e736abae0cc7625fe6@%3Cdev.felix.apache.org%3E
https://www.oracle.com/security-alerts/cpujan2021.html
https://packetstormsecurity.com/files/162160/jQuery-1.0.3-Cross-Site-Scripting.html
https://lists.apache.org/thread.html/r706cfbc098420f7113968cc377247ec3d1439bce42e679c11c609e2d@%3Cissues.flink.apache.org%3E
https://lists.apache.org/thread.html/ra3c9219fcb0b289e18e9ec5a5ebeaa5c17d6b79a201667675af6721c@%3Cgitbox.hive.apache.org%3E
https://lists.apache.org/thread.html/r0483ba0072783c2e1bfea613984bfb3c86e73ba8879d780dc1cc7d36@%3Cissues.flink.apache.org%3E
https://lists.apache.org/thread.html/rab82dd040f302018c85bd07d33f5604113573514895ada523c3401d9@%3Ccommits.hive.apache.org%3E
https://www.oracle.com/security-alerts/cpuapr2022.html
http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00067.html
http://lists.opensuse.org/opensuse-security-announce/2020-11/msg00039.html
https://www.oracle.com/security-alerts/cpuoct2021.html
https://lists.apache.org/thread.html/rd38b4185a797b324c8dd940d9213cf99fcdc2dbf1fc5a63ba7dee8c9@%3Cissues.hive.apache.org%3E
https://lists.apache.org/thread.html/r3702ede0ff83a29ba3eb418f6f11c473d6e3736baba981a8dbd9c9ef@%3Cdev.felix.apache.org%3E
https://lists.apache.org/thread.html/r8f70b0f65d6bedf316ecd899371fd89e65333bc988f6326d2956735c@%3Cissues.flink.apache.org%3E
http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00085.html
https://lists.apache.org/thread.html/rbb448222ba62c430e21e13f940be4cb5cfc373cd3bce56b48c0ffa67@%3Cdev.flink.apache.org%3E
https://www.oracle.com/security-alerts/cpujan2022.html
https://lists.apache.org/thread.html/r9c5fda81e4bca8daee305b4c03283dddb383ab8428a151d4cb0b3b15@%3Cissues.hive.apache.org%3E
https://lists.apache.org/thread.html/rf1ba79e564fe7efc56aef7c986106f1cf67a3427d08e997e088e7a93@%3Cgitbox.hive.apache.org%3E
https://lists.apache.org/thread.html/r2c85121a47442036c7f8353a3724aa04f8ecdfda1819d311ba4f5330@%3Cdev.felix.apache.org%3E
https://jquery.com/upgrade-guide/3.5/
https://lists.apache.org/thread.html/r9e0bd31b7da9e7403478d22652b8760c946861f8ebd7bd750844898e@%3Cdev.felix.apache.org%3E
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AVKYXLWCLZBV2N7M46KYK4LVA5OXWPBY/
https://lists.apache.org/thread.html/ra374bb0299b4aa3e04edde01ebc03ed6f90cf614dad40dd428ce8f72@%3Cgitbox.hive.apache.org%3E
https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6
https://www.tenable.com/security/tns-2021-10
https://www.tenable.com/security/tns-2021-02
https://lists.apache.org/thread.html/r54565a8f025c7c4f305355fdfd75b68eca442eebdb5f31c2e7d977ae@%3Cissues.flink.apache.org%3E
https://lists.apache.org/thread.html/rb69b7d8217c1a6a2100247a5d06ce610836b31e3f5d73fc113ded8e7@%3Cissues.hive.apache.org%3E

https://lists.apache.org/thread.html/r564585d97bc069137e64f521e68ba490c7c9c5b342df5d73c49a0760@%3Cissues.flink.apache.org%3E
https://www.oracle.com/security-alerts/cpuApr2021.html
https://blog.jquery.com/2020/04/10/jquery-3-5-0-released
https://lists.apache.org/thread.html/rede9cfaa756e050a3d83045008f84a62802fc68c17f2b4eabeaae5e4@%3Cissues.flink.apache.org%3E
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SAPQVX3XDNPGFT26QAQ6AJIXZZBZ4CD4/
https://www.drupal.org/sa-core-2020-002
https://lists.apache.org/thread.html/r6c4df3b33e625a44471009a172dabe6865faec8d8f21cac2303463b1@%3Cissues.hive.apache.org%3E
https://lists.apache.org/thread.html/ree3bd8ddb23df5fa4e372d11c226830ea3650056b1059f3965b3fce2@%3Cissues.flink.apache.org%3E
https://lists.apache.org/thread.html/r6e97b37963926f6059ecc1e417721608723a807a76af41d4e9dbed49@%3Cissues.hive.apache.org%3E
https://lists.apache.org/thread.html/r1fed19c860a0d470f2a3eded12795772c8651ff583ef951ddac4918c@%3Cgitbox.hive.apache.org%3E
https://lists.apache.org/thread.html/rda99599896c3667f2cc9e9d34c7b6ef5d2bbed1f4801e1d75a2b0679@%3Ccommits.nifi.apache.org%3E
https://lists.apache.org/thread.html/rf661a90a15da8da5922ba6127b3f5f8194d4ebec8855d60a0dd13248@%3Cdev.hive.apache.org%3E
https://lists.apache.org/thread.html/rf0f8939596081d84be1ae6a91d6248b96a02d8388898c372ac807817@%3Cdev.felix.apache.org%3E
https://lists.apache.org/thread.html/re4ae96fa5c1a2fe71ccbb7b7ac1538bd0cb677be270a2bf6e2f8d108@%3Cissues.flink.apache.org%3E
https://www.debian.org/security/2020/dsa-4693
https://www.oracle.com//security-alerts/cpujul2021.html
https://lists.apache.org/thread.html/r094f435595582f6b5b24b66fedf80543aa8b1d57a3688fbcc21f06ec@%3Cissues.hive.apache.org%3E
https://lists.apache.org/thread.html/ra32c7103ded9041c7c1cb8c12c8d125a6b2f3f3270e2937ef8417fac@%3Cgitbox.hive.apache.org%3E
https://lists.apache.org/thread.html/r9006ad2abf81d02a0ef2126bab5177987e59095b7194a487c4ea247c@%3Ccommits.felix.apache.org%3E
https://www.oracle.com/security-alerts/cpujul2020.html
https://www.cybersecurity-help.cz/vdb/SB2021110301
https://packetstormsecurity.com/files/159513/Red-Hat-Security-Advisory-2020-4211-01.html
https://www.oracle.com/security-alerts/cpuapr2021.html
https://www.oracle.com/security-alerts/cpuoct2021.html
https://www.ibm.com/blogs/psirt/security-bulletin-ibm-kenexa-lcms-premier-on-premise-all-jquery-publicly-disclosed-vulnerability-cve-2020-11023-cve-2020-11022/
https://www.auscert.org.au/bulletins/ESB-2020.4248/
https://www.cybersecurity-help.cz/vdb/SB2022011837
https://www.auscert.org.au/bulletins/ESB-2021.3823
https://www.auscert.org.au/bulletins/ESB-2020.2287/
https://packetstormsecurity.com/files/158797/Red-Hat-Security-Advisory-2020-3369-01.html
https://packetstormsecurity.com/files/161727/Red-Hat-Security-Advisory-2021-0778-01.html
https://packetstormsecurity.com/files/159275/Red-Hat-Security-Advisory-2020-3807-01.html

https://packetstormsecurity.com/files/162160/jQuery-1.0.3-Cross-Site-Scripting.html

https://www.oracle.com/security-alerts/cpujul2021.html

https://packetstormsecurity.com/files/161830/Red-Hat-Security-Advisory-2021-0860-01.html

https://www.exploit-db.com/exploits/49767

https://nvd.nist.gov/vuln/detail/CVE-2020-11023

https://packetstormsecurity.com/files/162651/Red-Hat-Security-Advisory-2021-1846-01.html

https://www.auscert.org.au/bulletins/ESB-2020.3875/

https://www.ibm.com/blogs/psirt/security-bulletin-jquery-vulnerabilities-affect-ibm-emptoris-strategic-supply-management-platform-cve-2020-11023-cve-2020-11022/

https://www.ibm.com/support/pages/node/6520510

https://packetstormsecurity.com/files/158555/Gentoo-Linux-Security-Advisory-202007-03.html

https://www.ibm.com/blogs/psirt/security-bulletin-jquery-as-used-by-ibm-qradar-network-packet-capture-is-vulnerable-to-cross-site-scripting-xss-cve-2020-11023-cve-2020-11022/

https://www.auscert.org.au/bulletins/ESB-2023.1653

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-is-vulnerable-to-using-components-with-known-vulnerabilities-10/

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-is-vulnerable-to-using-components-with-known-vulnerabilities-8/

https://www.auscert.org.au/bulletins/ESB-2021.0923

https://www.auscert.org.au/bulletins/ESB-2020.2694/

https://packetstormsecurity.com/files/158282/Red-Hat-Security-Advisory-2020-2813-01.html

https://www.auscert.org.au/bulletins/ESB-2020.2375/

https://www.auscert.org.au/bulletins/ESB-2021.0845

https://www.oracle.com/security-alerts/cpuoct2020.html

https://www.auscert.org.au/bulletins/ESB-2020.2775/

https://www.auscert.org.au/bulletins/ESB-2021.1066

https://www.ibm.com/blogs/psirt/security-bulletin-vulnerabilities-in-jquery-affect-ibm-license-metric-tool-v9/

https://www.auscert.org.au/bulletins/ESB-2022.5150

https://packetstormsecurity.com/files/168304/Red-Hat-Security-Advisory-2022-6393-01.html

https://www.auscert.org.au/bulletins/ESB-2020.1804/

https://packetstormsecurity.com/files/160274/Red-Hat-Security-Advisory-2020-5249-01.html

https://www.auscert.org.au/bulletins/ESB-2022.0824

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-security-verify-information-queue-uses-a-node-js-package-with-known-vulnerabilities-cve-2020-11023-cve-2020-11022/

https://www.cybersecurity-help.cz/vdb/SB2021042101

https://www.auscert.org.au/bulletins/ESB-2020.1961/

https://www.auscert.org.au/bulletins/ESB-2022.1512

https://www.ibm.com/blogs/psirt/security-bulletin-cross-site-scripting-vulnerabilities-in-jquery-might-affect-ibm-business-automation-workflow-and-ibm-business-process-manager-bpm-cve-2020-7656-cve-2020-11022-cve-2020-11023-2/

http://www.nsfocus.net/vulndb/48902

https://support.lenovo.com/us/en/product_security/LEN-60182

https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilites-affect-ibm-jazz-foundation-and-ibm-engineering-products-5/

https://www.cybersecurity-help.cz/vdb/SB2022022516

https://packetstormsecurity.com/files/158750/Red-Hat-Security-Advisory-2020-3247-01.html

https://www.ibm.com/blogs/psirt/security-bulletin-jquery-as-used-in-ibm-security-qradar-packet-capture-is-vulnerable-to-cross-site-scripting-xss-cve-2020-11023-cve-2020-11022/

https://www.auscert.org.au/bulletins/ESB-2021.1703
https://www.auscert.org.au/bulletins/ESB-2020.2714/
https://www.ibm.com/support/pages/node/6525182
https://packetstormsecurity.com/files/158406/Red-Hat-Security-Advisory-2020-2412-01.html
https://www.ibm.com/blogs/psirt/security-bulletin-ibm-tivoli-netcool-impact-is-affected-by-jquery-vulnerabilities-cve-2020-11022-cve-2020-11023/
https://packetstormsecurity.com/files/160548/Red-Hat-Security-Advisory-2020-5412-01.html
https://www.auscert.org.au/bulletins/ESB-2020.2660.3/
https://www.ibm.com/blogs/psirt/security-bulletin-ibm-api-connect-is-impacted-by-vulnerabilities-in-drupal-cve-2020-11022-cve-2020-11023/
https://www.ibm.com/blogs/psirt/security-bulletin-ibm-kenexa-lms-on-premise-all-jquery-publicly-disclosed-vulnerability-cve-2020-11023-cve-2020-11022/
https://www.ibm.com/blogs/psirt/security-bulletin-ibm-planning-analytics-workspace-is-affected-by-security-vulnerabilities-3/
https://www.auscert.org.au/bulletins/ESB-2020.1863/
https://www.ibm.com/blogs/psirt/security-bulletin-ibm-api-connect-is-impacted-by-vulnerabilities-in-drupal-cve-2020-11022-cve-2020-11023-2/
https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-jquery-fixed-in-mobile-foundation-cve-2020-11023-cve-2020-11022/
https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-jquery-affect-ibm-wiotp-messagegateway-cve-2020-11023-cve-2020-11022/
https://www.auscert.org.au/bulletins/ESB-2020.3700/
https://www.auscert.org.au/bulletins/ESB-2021.1916
https://www.auscert.org.au/bulletins/ESB-2021.1519
https://www.cybersecurity-help.cz/vdb/SB2022072027
https://www.auscert.org.au/bulletins/ESB-2021.0909
https://www.ibm.com/blogs/psirt/security-bulletin-security-vulnerabilities-have-been-fixed-in-ibm-security-identity-manager-virtual-appliance/
https://www.cybersecurity-help.cz/vdb/SB2021052207
https://packetstormsecurity.com/files/170821/Red-Hat-Security-Advisory-2023-0552-01.html
https://www.auscert.org.au/bulletins/ESB-2023.0585
https://packetstormsecurity.com/files/159852/Red-Hat-Security-Advisory-2020-4847-01.html
https://www.auscert.org.au/bulletins/ESB-2021.2525
https://www.auscert.org.au/bulletins/ESB-2020.2660/
https://www.auscert.org.au/bulletins/ESB-2020.4421/
https://www.auscert.org.au/bulletins/ESB-2021.0620
https://www.auscert.org.au/bulletins/ESB-2023.1351
https://www.auscert.org.au/bulletins/ESB-2023.0583
https://www.ibm.com/blogs/psirt/security-bulletin-ibm-license-key-server-administration-and-reporting-tool-is-impacted-by-multiple-vulnerabilities-in-jquery-bootstrap-and-angularjs/
https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerability-issues-affect-ibm-spectrum-symphony-7-3-1/
https://www.cybersecurity-help.cz/vdb/SB2022012403
https://www.ibm.com/blogs/psirt/security-bulletin-vulnerabilities-in-jquery-spring-dom4j-mongodb-linux-kernel-targetcli-fb-jackson-node-js-and-apache-commons-affect-ibm-spectrum-protect-plus/
https://www.cybersecurity-help.cz/vdb/SB2021072824
https://www.ibm.com/blogs/psirt/security-bulletin-cross-site-scripting-vulnerabilities-in-jquery-might-affect-ibm-business-automation-workflow-and-ibm-business-process-manager-bpm-cve-2020-7656-cve-2020-11022-cve-2020-11023/
https://www.auscert.org.au/bulletins/ESB-2021.3663

	https://us-cert.cisa.gov/ics/advisories/icsa-22-097-01 https://www.auscert.org.au/bulletins/ESB-2020.3255/ https://packetstormsecurity.com/files/164887/Red-Hat-Security-Advisory-2021-4142-02.html https://www.ibm.com/blogs/psirt/security-bulletin-security-vulnerability-has-been-identified-in-bigfix-platform-shipped-with-ibm-license-metric-tool-2/ https://packetstormsecurity.com/files/170823/Red-Hat-Security-Advisory-2023-0553-01.html https://www.auscert.org.au/bulletins/ESB-2020.3485/
CVE	CVE-2020-11023
CVSS	6.1
CNCVE	CNCVE-202011023
CNNVD	CNNVD-202004-2420
检测详情	主机：10.129.57.55| 端口：18080| 服务：http| 协议：TCP jquery:jquery 1.12.4 >= 1.0.3 and jquery:jquery 1.12.4 < 3.5.0 漏洞状态：新增

⊟ jQuery 跨站脚本漏洞（CVE-2020-11022） | 跨站脚本 | 中风险 | 1

漏洞编号	1144197
风险级别	中风险
概要	
描述	jQuery是美国John Resig个人开发者的一套开源、跨浏览器的JavaScript库。该库简化了HTML与JavaScript之间的操作，并具有模块化、插件扩展等特点。 jQuery 1.2版本至3.5.0之前版本中存在跨站脚本漏洞。该漏洞源于WEB应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。
解决办法	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
详情请参阅	https://github.com/jquery/jquery/commit/1d61fd9407e6fbe82fe55cb0b938307aa0791f77 https://lists.apache.org/thread.html/r8f70b0f65d6bedf316ecd899371fd89e65333bc988f6326d2956735c@%3Cissues.flink.apache.org%3E http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00085.html https://lists.apache.org/thread.html/rbb448222ba62c430e21e13f940be4cb5cfc373cd3bce56b48c0ffa67@%3Cdev.flink.apache.org%3E https://www.oracle.com/security-alerts/cpujan2022.html https://security.gentoo.org/glsa/202007-03 https://jquery.com/upgrade-guide/3.5/ https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AVKYXLWCLZBV2N7M46KYK4LVA5OXWPBY/ https://lists.apache.org/thread.html/r49ce4243b4738dd763caeb27fa8ad6afb426ae3e8c011ff00b8b1f48@%3Cissues.flink.apache.org%3E https://security.netapp.com/advisory/ntap-20200511-0006/ https://www.oracle.com/security-alerts/cpujul2022.html https://www.oracle.com/security-alerts/cpuoct2020.html https://www.tenable.com/security/tns-2021-10

https://www.tenable.com/security/tns-2020-11
https://www.tenable.com/security/tns-2021-02
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/VOE7P7APPRQKD4FGNHBKJPDY6FFCOH3W/
https://lists.debian.org/debian-lts-announce/2021/03/msg00033.html
https://lists.apache.org/thread.html/r54565a8f025c7c4f305355fdfd75b68eca442eebdb5f31c2e7d977ae@%3Cissues.flink.apache.org%3E
https://lists.apache.org/thread.html/rdf44341677cf7eec7e9aa96dcf3f37ed709544863d619cca8c36f133@%3Ccommits.airflow.apache.org%3E
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SFP4UK4EGP4AFH2MWYJ5A5Z4I7XVFQ6B/
https://lists.apache.org/thread.html/r564585d97bc069137e64f521e68ba490c7c9c5b342df5d73c49a0760@%3Cissues.flink.apache.org%3E
https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
https://www.oracle.com/security-alerts/cpuApr2021.html
https://packetstormsecurity.com/files/162159/jQuery-1.2-Cross-Site-Scripting.html
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/QPN2L2XVQGUA2V5HNQJWHK3APSK3VN7K/
https://lists.apache.org/thread.html/rede9cfaa756e050a3d83045008f84a62802fc68c17f2b4eabeaae5e4@%3Cissues.flink.apache.org%3E
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SAPQVX3XDNPGFT26QAQ6AJIXZZBZ4CD4/
https://www.drupal.org/sa-core-2020-002
https://www.oracle.com/security-alerts/cpujan2021.html
https://lists.apache.org/thread.html/ree3bd8ddb23df5fa4e372d11c226830ea3650056b1059f3965b3fce2@%3Cissues.flink.apache.org%3E
https://lists.apache.org/thread.html/r706cfbc098420f7113968cc377247ec3d1439bce42e679c11c609e2d@%3Cissues.flink.apache.org%3E
https://www.tenable.com/security/tns-2020-10
https://lists.apache.org/thread.html/r0483ba0072783c2e1bfea613984bfb3c86e73ba8879d780dc1cc7d36@%3Cissues.flink.apache.org%3E
https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2
https://lists.apache.org/thread.html/re4ae96fa5c1a2fe71ccbb7b7ac1538bd0cb677be270a2bf6e2f8d108@%3Cissues.flink.apache.org%3E
https://www.debian.org/security/2020/dsa-4693
https://www.oracle.com//security-alerts/cpujul2021.html
https://www.oracle.com/security-alerts/cpuapr2022.html
http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00067.html
http://lists.opensuse.org/opensuse-security-announce/2020-11/msg00039.html
https://www.oracle.com/security-alerts/cpuoct2021.html
https://www.oracle.com/security-alerts/cpujul2020.html
https://www.oracle.com/security-alerts/cpujul2020.html
https://www.cybersecurity-help.cz/vdb/SB2022041931
https://packetstormsecurity.com/files/161727/Red-Hat-Security-Advisory-2021-0778-01.html
https://packetstormsecurity.com/files/159275/Red-Hat-Security-Advisory-2020-3807-01.html
https://www.oracle.com/security-alerts/cpujul2021.html
https://www.exploit-db.com/exploits/49766

http://www.nsfocus.net/vulndb/48898

https://www.auscert.org.au/bulletins/ESB-2020.3875/

https://www.ibm.com/blogs/psirt/security-bulletin-jquery-vulnerabilities-affect-ibm-emptoris-strategic-supply-management-platform-cve-2020-11023-cve-2020-11022/

https://www.ibm.com/support/pages/node/6520510

https://packetstormsecurity.com/files/158555/Gentoo-Linux-Security-Advisory-202007-03.html

https://www.ibm.com/blogs/psirt/security-bulletin-jquery-as-used-by-ibm-qradar-network-packet-capture-is-vulnerable-to-cross-site-scripting-xss-cve-2020-11023-cve-2020-11022/

https://www.cybersecurity-help.cz/vdb/SB2021072292

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-is-vulnerable-to-using-components-with-known-vulnerabilities-10/

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-is-vulnerable-to-using-components-with-known-vulnerabilities-8/

https://www.auscert.org.au/bulletins/ESB-2020.2375/

https://www.auscert.org.au/bulletins/ESB-2021.1066

https://www.auscert.org.au/bulletins/ESB-2022.5150

https://packetstormsecurity.com/files/168304/Red-Hat-Security-Advisory-2022-6393-01.html

https://www.cybersecurity-help.cz/vdb/SB2021042543

https://www.auscert.org.au/bulletins/ESB-2020.1804/

https://www.auscert.org.au/bulletins/ESB-2020.1925/

https://www.cybersecurity-help.cz/vdb/SB2021042302

https://packetstormsecurity.com/files/160274/Red-Hat-Security-Advisory-2020-5249-01.html

https://www.cybersecurity-help.cz/vdb/SB2021072721

https://www.cybersecurity-help.cz/vdb/SB2022022516

https://packetstormsecurity.com/files/157850/Red-Hat-Security-Advisory-2020-2217-01.html

https://www.cybersecurity-help.cz/vdb/SB2022072094

https://www.cybersecurity-help.cz/vdb/SB2021101936

https://packetstormsecurity.com/files/158406/Red-Hat-Security-Advisory-2020-2412-01.html

https://www.auscert.org.au/bulletins/ESB-2020.2660.3/

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-kenexa-lms-on-premise-all-jquery-publicly-disclosed-vulnerability-cve-2020-11023-cve-2020-11022/

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-planning-analytics-workspace-is-affected-by-security-vulnerabilities-3/

https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-jquery-affect-ibm-wiotp-messagegateway-cve-2020-11023-cve-2020-11022/

https://www.oracle.com/security-alerts/cpujan2021.html

https://www.auscert.org.au/bulletins/ESB-2021.1916

https://www.auscert.org.au/bulletins/ESB-2021.1519

https://packetstormsecurity.com/files/170821/Red-Hat-Security-Advisory-2023-0552-01.html

https://www.auscert.org.au/bulletins/ESB-2023.0585

https://packetstormsecurity.com/files/159852/Red-Hat-Security-Advisory-2020-4847-01.html

https://www.auscert.org.au/bulletins/ESB-2020.2660/

https://www.auscert.org.au/bulletins/ESB-2023.0583

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-license-key-server-administration-and-reporting-tool-is-impacted-by-multiple-vulnerabilities-in-jquery-bootstrap-and-angularjs/

https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerability-issues-affect-ibm-spectrum-symphony-7-3-1/

https://www.ibm.com/blogs/psirt/security-bulletin-cross-site-scripting-vulnerabilities-in-jquery-might-affect-ibm-business-automation-workflow-and-ibm-business-process-manager-bpm-cve-2020-7656-cve-2020-11022-cve-2020-11023/

https://www.auscert.org.au/bulletins/ESB-2020.3255/

https://www.auscert.org.au/bulletins/ESB-2020.3485/

https://packetstormsecurity.com/files/162159/jQuery-1.2-Cross-Site-Scripting.html

https://packetstormsecurity.com/files/159513/Red-Hat-Security-Advisory-2020-4211-01.html

https://www.oracle.com/security-alerts/cpuapr2021.html

https://www.oracle.com/security-alerts/cpuoct2021.html

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-kenexa-lcms-premier-on-premise-all-jquery-publicly-disclosed-vulnerability-cve-2020-11023-cve-2020-11022/

https://www.auscert.org.au/bulletins/ESB-2020.4248/

https://www.auscert.org.au/bulletins/ESB-2020.2287/

https://www.oracle.com/security-alerts/cpuapr2022.html

https://www.auscert.org.au/bulletins/ESB-2020.2966/

https://nvd.nist.gov/vuln/detail/CVE-2020-11022

https://packetstormsecurity.com/files/157905/Red-Hat-Security-Advisory-2020-2362-01.html

https://www.auscert.org.au/bulletins/ESB-2020.1880/

https://www.auscert.org.au/bulletins/ESB-2023.1653

https://www.auscert.org.au/bulletins/ESB-2020.2694/

https://www.cybersecurity-help.cz/vdb/SB2022042537

https://packetstormsecurity.com/files/158282/Red-Hat-Security-Advisory-2020-2813-01.html

https://www.cybersecurity-help.cz/vdb/SB2021042618

https://www.auscert.org.au/bulletins/ESB-2021.0845

https://www.oracle.com/security-alerts/cpuoct2020.html

https://www.auscert.org.au/bulletins/ESB-2020.2775/

https://www.ibm.com/blogs/psirt/security-bulletin-vulnerabilities-in-jquery-affect-ibm-license-metric-tool-v9/

https://www.auscert.org.au/bulletins/ESB-2022.0824

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-security-verify-information-queue-uses-a-node-js-package-with-known-vulnerabilities-cve-2020-11023-cve-2020-11022/

https://www.auscert.org.au/bulletins/ESB-2020.1961/

https://www.auscert.org.au/bulletins/ESB-2022.1512

https://www.ibm.com/blogs/psirt/security-bulletin-cross-site-scripting-vulnerabilities-in-jquery-might-affect-ibm-business-automation-workflow-and-ibm-business-process-manager-bpm-cve-2020-7656-cve-2020-11022-cve-2020-11023-2/

https://packetstormsecurity.com/files/159353/Red-Hat-Security-Advisory-2020-3936-01.html

https://support.lenovo.com/us/en/product_security/LEN-60182

https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilites-affect-ibm-jazz-foundation-and-ibm-engineering-products-5/

https://www.auscert.org.au/bulletins/ESB-2020.3028/

https://cxsecurity.com/issue/WLB-2022060033

https://www.auscert.org.au/bulletins/ESB-2021.2515

https://packetstormsecurity.com/files/158750/Red-Hat-Security-Advisory-2020-3247-01.html

https://www.ibm.com/blogs/psirt/security-bulletin-jquery-as-used-in-ibm-security-qradar-packet-capture-is-vulnerable-to-cross-site-scripting-xss-cve-2020-11023-cve-2020-11022/

https://www.cybersecurity-help.cz/vdb/SB2022012754

https://www.auscert.org.au/bulletins/ESB-2021.0465

https://www.ibm.com/support/pages/node/6525182

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-tivoli-netcool-impact-is-affected-by-jquery-vulnerabilities-cve-2020-11022-cve-2020-11023/

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-api-connect-is-impacted-by-vulnerabilities-in-drupal-cve-2020-11022-cve

	-2020-11023/ https://www.ibm.com/support/pages/node/6490381 https://www.auscert.org.au/bulletins/ESB-2020.1863/ https://www.ibm.com/blogs/psirt/security-bulletin-ibm-api-connect-is-impacted-by-vulnerabilities-in-drupal-cve-2020-11022-cve-2020-11023-2/ https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-jquery-fixed-in-mobile-foundation-cve-2020-11023-cve-2020-11022/ https://www.auscert.org.au/bulletins/ESB-2020.3700/ https://www.cybersecurity-help.cz/vdb/SB2022071412 https://www.auscert.org.au/bulletins/ESB-2021.0909 https://www.ibm.com/blogs/psirt/security-bulletin-security-vulnerabilities-have-been-fixed-in-ibm-security-identity-manager-virtual-appliance/ https://www.auscert.org.au/bulletins/ESB-2020.3902/ https://www.auscert.org.au/bulletins/ESB-2021.2525 https://www.auscert.org.au/bulletins/ESB-2021.0620 https://www.cybersecurity-help.cz/vdb/SB2022012403 https://www.ibm.com/blogs/psirt/security-bulletin-vulnerabilities-in-jquery-spring-dom4j-mongodb-linux-kernel-targetcli-fb-jackson-node-js-and-apache-commons-affect-ibm-spectrum-protect-plus/ https://us-cert.cisa.gov/ics/advisories/icsa-22-097-01 https://www.ibm.com/blogs/psirt/security-bulletin-security-vulnerability-has-been-identified-in-bigfix-platform-shipped-with-ibm-license-metric-tool-2/ https://www.auscert.org.au/bulletins/ESB-2020.3368/ https://packetstormsecurity.com/files/170823/Red-Hat-Security-Advisory-2023-0553-01.html
CVE	CVE-2020-11022
CVSS	6.1
CNCVE	CNCVE-202011022
CNNVD	CNNVD-202004-2429
检测详情	主机：10.129.57.55| 端口：18080| 服务：http| 协议：TCP jquery:jquery 1.12.4 >= 1.2 and jquery:jquery 1.12.4 < 3.5.0 漏洞状态：新增

ICMP时间戳检测	默认探测	低风险	1

漏洞编号	39248
风险级别	低风险
概要	远程信息泄露
描述	远程主机响应了ICMP时间戳请求。时间戳回复是一种ICMP消息，它回复时间戳消息。它由时间戳的发送方发送的始发时间戳以及接收时间戳和发送时间戳组成。从理论上讲，该信息可用于开发其他服务中基于弱时间的随机数生成器。
解决办法	建议添加防火墙策略过滤ICMP timestamp进出报文。
详情请参阅	URL:http://www.ietf.org/rfc/rfc0792.txt
CVE	CVE-1999-0524
CVSS	2.1
CNCVE	CNCVE-19990524

检测详情	主机：10.129.57.55 漏洞状态：新增

允许Traceroute探测	默认探测	信息	1

漏洞编号	38231
风险级别	信息
概要	
描述	检测出可使用Traceroute获取扫描器与远程主机间的路由信息。
解决办法	建议防火墙上配置禁用策略
CVSS	0.0
检测详情	主机：10.129.57.55 Here is the route from 10.129.32.98 to 10.129.57.55:10.129.32.98? 漏洞状态：新增

远程主机Web服务404检查【原理扫描】	Web应用	信息	1

漏洞编号	55223
风险级别	信息
概要	
描述	远程Web服务器不回复404错误代码。此Web服务器配置不当，是因为当请求不存在的文件时，它不返回“ 404 Not Found”错误代码，而可能返回站点地图，搜索页面或身份验证页面。
解决办法	信息探测，无需修复
CVSS	0.0
检测详情	主机：10.129.57.55| 端口：18080| 服务：http| 协议：TCP 远程主机Web服务404检查 漏洞状态：新增

探测到jquery	其它	信息	1

漏洞编号	55510
风险级别	信息
概要	
描述	检测到远程主机使用了jquery
解决办法	通过加固软件的配置，禁止Banner信息的泄露，从而防止服务版本的泄露
CVSS	0.0
检测详情	主机：10.129.57.55| 端口：18080| 服务：http|

	协议：TCP
	jquery version: 1.12.4 detected from /static/component/jquery-1.12.4.js
	漏洞状态：新增

5 WEB漏洞信息

5.1 WEB漏洞统计概况

5.1.1 漏洞等级分布

高风险	中风险	低风险	信息级	总计
0	0	0	0	0

5.1.2 漏洞类别统计

序号	WEB漏洞类别	总计

5.1.3 漏洞排名

序号	WEB漏洞名称（TOP10）	总计

5.2 WEB漏洞详情

漏洞名称	漏洞分类	漏洞类型	出现次数

6 弱口令

序号	主机地址	用户名	密码	服务	端口

7 参考标准

7.1 单一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
高	7 <= 漏洞风险值 <= 10	攻击者可以访问机密信息、破坏或删除数据且可以制造系统中断。
中	4 <= 漏洞风险值 < 7	攻击者可访问部分受限的信息、可以破坏信息且可以禁用网络中的个体目标系统。
低	0 < 漏洞风险值 < 4	攻击者可以在特殊情况下访问不受限的信息、破坏或损坏信息但无法制造任何系统中断。
信息	漏洞风险值 = 0	攻击者可以获取服务及组件等版本信息。

1. 可远程获取漏洞组件的版本信息。
2. 目标系统服务器开放了不必要的服务。
3. 可远程访问到某些不在目录树中的文件或读取服务器动态脚本的源码。
4. 可远程因为会话管理的问题导致身份冒用。
5. 可远程利用受影响的系统服务器攻击其他浏览网站的用户。
6. 可远程读取系统文件或后台数据库。
7. 可远程读写系统文件、操作后台数据库。
8. 可远程以普通用户身份执行命令或进行拒绝服务攻击。
9. 可远程以管理用户身份执行命令（受限、不太容易利用）。
10. 可远程以管理用户身份执行命令（不受限、容易利用）。

7.2 资产风险等级评定标准

资产风险等级	资产风险值区域
非常危险	8 <= 资产风险值 <= 10
比较危险	5 <= 资产风险值 < 8
比较安全	2 <= 资产风险值 < 5
非常安全	0 <= 资产风险值 < 2

1. 将资产的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。
2. 单个资产的风险值按照风险评估模型计算来得到；网络的风险值是由最危险资产决定，即最大的资产风险值。
3. 高、中、低漏洞威胁的定义参见《单一漏洞风险等级评定标准》。
4. 资产的风险等级定位为四级：非常危险、比较危险、比较安全和非常安全。具体的评判标准请参考《资产风险等级评定标准》。

8 安全建议

随着越来越多的网络访问通过系统漏洞进行操作，系统漏洞已成为互联网安全的一个热点，基于系统漏洞的攻击广为流行，CGI攻击检测、网络设备和防火墙、本地安全检查等问题严重威胁着系统管理者和系统用户的安全，我们有必要采取措施消除这些风险。

建议对存在漏洞的资产参考附件中提出的解决方案进行漏洞修补、安全增强。

请专业的安全研究人员或安全公司对系统架构做全面的安全审计，修补所有发现的安全漏洞，这种白盒安全测试比较深入全面。

对系统的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。

采用专业的系统安全产品，可以在不修改系统本身的情况下对大多数的基于漏洞攻击起到有效的阻断作用。

建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的高危漏洞，特别是影响到漏洞站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。

9 联系我们

公司：奇安信网神信息技术（北京）股份有限公司

网址：www.qianxin.com

热线：010-62972893

传真：

地址：北京市西城区西直门外南路26号院1号楼2层