北京师范大学网络信息安全通告

2021 年 1 月报告

北京师范大学信息网络中心

2021 年 2 月

目录

漏洞态势 2
1. 公开漏洞情况 2
1.1. 漏洞增长概况 2
1.2. 漏洞分布情况 3
1.2.1. 漏洞厂商分布 3
1.2.2. 漏洞产品分布 3
1.2.3. 漏洞类型分布 4
1.2.4. 漏洞危害等级分布 5
1.3. 漏洞修复情况 6
1.3.1. 整体修复情况 6
1.3.2. 厂商修复情况 6
1.4. 重要漏洞实例 7
1.4.1. 超危漏洞实例 7
1.4.2. 高危漏洞实例 13
2. 接报漏洞情况 28
3. 重大漏洞预警 31
3.1. SonicWall SSL-VPN 安全漏洞的预警 31
3.2. 致远OA文件上传漏洞的预警 32

漏洞态势

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2020 年 13 月份新增安全漏洞共 1545 个，从厂商分布来看，思科公司产品的漏洞数量最多，共发布 154 个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到 13.79%。本月新增漏洞中，超危漏洞 151 个、高危漏洞 659 个、中危漏洞 714 个、低危漏洞 21 个，相应修复率分别为 85.43%、92.11%、85.29%以及 95.24%。合计 1365 个漏洞已有修复补丁发布，本月整体修复率 88.35%。

截至 2021 年 01 月 31 日，CNNVD 采集漏洞总量已达 157269 个。

1.1 漏洞增长概况

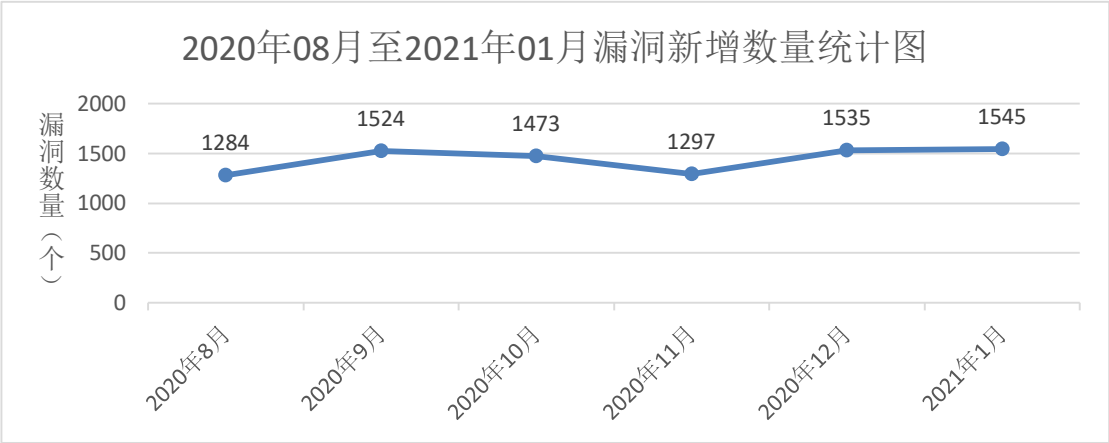

图 1 2020 年 8 月至 2021 年 1 月漏洞新增数量统计图

2021 年 1 月新增安全漏洞 1545 个，与上月（1535 个）相比增加了 0.65%。根据近 6 个月来漏洞新增数量统计图，平均每月漏洞数量达到 1443 个。

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

1 月厂商漏洞数量分布情况如表 1 所示，思科公司漏洞达到 154 个，占本月漏洞总量的 9.97%。

表 1　2021 年 1 月排名前十厂商新增安全漏洞统计表

序号	厂商名称	漏洞数量	所占比例
1	思科	154	9.97%
2	Oracle	136	8.80%
3	IBM	84	5.44%
4	微软	83	5.37%
5	谷歌	69	4.47%
6	Mozilla 基金会	44	2.85%
7	西门子	30	1.94%
8	Qualcomm	27	1.75%
9	SAP	25	1.62%
10	惠普	21	1.36%

1.2.2 漏洞产品分布

1 月主流操作系统的漏洞统计情况如表 2 所示。本月 Windows 10 漏洞数量最多，共 64 个，占主流操作系统漏洞总量的 13.39%，排名第一。

表 2　2021 年 1 月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量
1	Windows 10	64

2	Windows Server 2019	55
3	Windows Server 2016	51
4	Windows Server 2012	43
5	Windows Server 2012 R2	43
6	Windows 8.1	43
7	Windows Rt 8.1	41
8	Windows 7	36
9	Windows Server 2008	36
10	Windows Server 2008 R2	36
11	Android	26
12	Linux Kernel	4
13	Apple Mac OS	0

1.2.3 漏洞类型分布

1 月份发布的漏洞类型分布如表 3 所示，其中缓冲区错误类漏洞所占比例最大，约为 13.79%。

表 3 2021 年 1 月漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	缓冲区错误	213	13.79%
2	跨站脚本	181	11.72%
3	代码问题	101	6.54%
4	访问控制错误	93	6.02%
5	信息泄露	80	5.18%
6	授权问题	72	4.66%
7	输入验证错误	62	4.01%
8	资源管理错误	55	3.56%
9	SQL 注入	37	2.39%
10	路径遍历	36	2.33%
11	跨站请求伪造	30	1.94%
12	注入	24	1.55%
13	命令注入	22	1.42%
14	操作系统命令注入	15	0.97%
15	竞争条件问题	12	0.78%
16	信任管理问题	11	0.71%
17	加密问题	11	0.71%
18	代码注入	7	0.45%
19	环境问题	6	0.39%
20	后置链接	5	0.32%

21	安全特征问题	4	0.26%
22	权限许可和访问控制问题	3	0.19%
23	数据伪造问题	3	0.19%
24	日志信息泄露	3	0.19%
25	数字错误	2	0.13%
26	默认配置问题	2	0.13%
27	处理逻辑错误	1	0.06%
28	配置错误	1	0.06%
29	格式化字符串错误	1	0.06%
30	其他	452	29.26%

1.2.4 漏洞危害等级分布

根据漏洞的影响范围、利用方式、攻击后果等情况，从高到低可将其分为四个危害等级，即超危、高危、中危和低危级别。13 月漏洞危害等级分布如图 2 所示，其中超危漏洞 151 条，占本月漏洞总数的 9.77%。

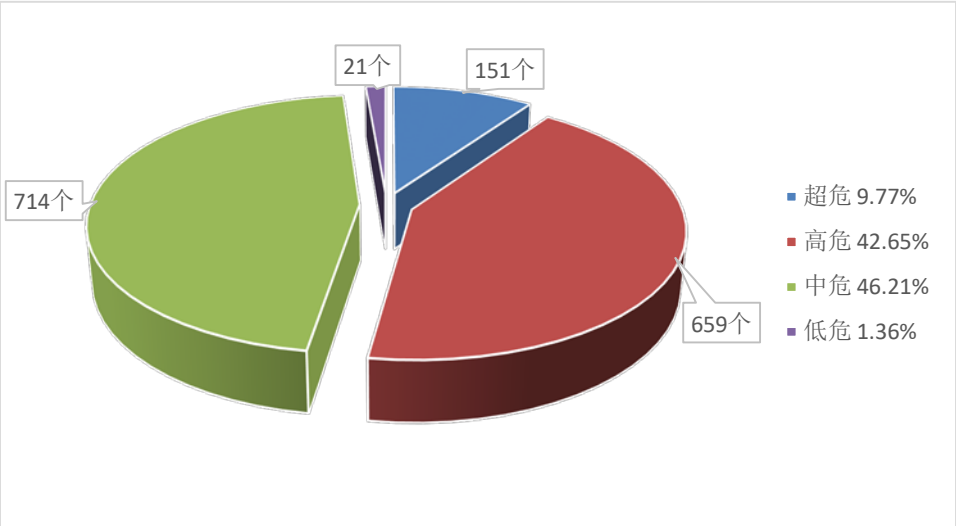

图 2　2021 年 1 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

1 月漏洞修复情况按危害等级进行统计见图 3。其中低危漏洞修复率最高，达到 95.24%，中危漏洞修复率最低，比例为 85.29%。总体来看，本月整体修复率，由上月的 83.26%上升至本月的 88.35%。

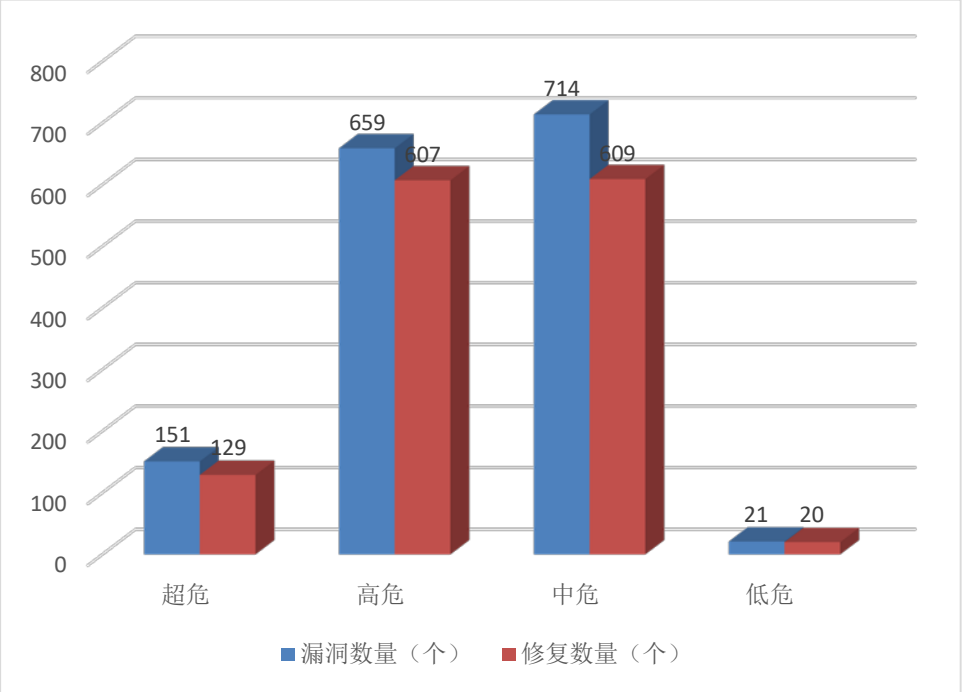

图 3　2021 年 1 月漏洞修复数量统计

1.3.2 厂商修复情况

1 月漏洞修复情况按漏洞数量前十厂商进行统计，其中思科、Oracle、IBM 等十个厂商共 673 条漏洞，占本月漏洞总数的 43.56%，漏洞修复率为 98.51%，详细情况见表 4。多数知名厂商对产品安全高度重视，产品漏洞修复比较及时，其中思科、Oracle、微软、西门子、Qualcomm、SAP、惠普等公司本月漏洞修复率均为 100%，共 663 条漏洞已全部修复。

表 4　2021 年 1 月厂商修复情况统计表

序号	厂商名称	漏洞数量（个）	修复数量	修复率
1	思科	154	154	100.00%
2	Oracle	136	136	100.00%
3	IBM	84	83	98.81%
4	微软	83	83	100.00%
5	谷歌	69	67	97.10%
6	Mozilla 基金会	44	37	84.09%
7	西门子	30	30	100.00%
8	Qualcomm	27	27	100.00%
9	SAP	25	25	100.00%
10	惠普	21	21	100.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 151 个，其中重要漏洞实例如表 5 所示。

表 5　2021 年 1 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	SQL 注入	CNNVD-202101-1516	Cisco	Cisco SD-WAN vManage Software SQL 注入漏洞（CNNVD-202101-1516）
		CNNVD-202101-1134	DELL	
		CNNVD-202101-522	Evolucare	
		CNNVD-202101-361	Fortinet	
		CNNVD-202101-1471	HGiga	
		CNNVD-202101-277	Ipeak	
		CNNVD-202101-263	Ispconfig 社区	
		CNNVD-202101-1587	Prestashop	
		CNNVD-202101-096	Projectworlds	
		CNNVD-202101-764	SAP	
		CNNVD-202101-2233	Spotweb 团队	
		CNNVD-202101-2234	个人开发者	
		CNNVD-202101-2326		
		CNNVD-202101-274		
		CNNVD-202101-909		
		CNNVD-202101-2347		
2	代码问题	CNNVD-202101-2043	Apache 基金会	Apache Dubbo 代码问题漏洞（CNNVD-202101-520）
		CNNVD-202101-520		
		CNNVD-202101-1301	HPE	

		CNNVD-202101-1114	Juniper Networks	
		CNNVD-202101-1074	Owasp 基金会	
		CNNVD-202101-349	Proofpoint	
		CNNVD-202101-351		
		CNNVD-202101-352		
		CNNVD-202101-489	Quest	
		CNNVD-202101-1289	Theonedev 团队	
		CNNVD-202101-1287		
		CNNVD-202101-1288		
		CNNVD-202101-025	Zend	
		CNNVD-202101-1322	个人开发者	
		CNNVD-202101-1096		
		CNNVD-202101-045		
3	授权问题	CNNVD-202101-037	Dell	Oracle Fusion Middleware WebLogic Server 授权问题漏洞 (CNNVD-202101-1343)
		CNNVD-202101-899	Facade	
		CNNVD-202101-1047	Loxone	
		CNNVD-202101-2580	Mitel Networks	
		CNNVD-202101-092	NEC	
		CNNVD-202101-1326	Oracle	
		CNNVD-202101-1343		
		CNNVD-202101-1445		
		CNNVD-202101-1356		
		CNNVD-202101-1148	Seeds	
		CNNVD-202101-369	Wordpress 基金会	
		CNNVD-202101-1469	个人开发者	
		CNNVD-202101-2346		
		CNNVD-202101-2430		
		CNNVD-202101-046	华硕	
4	操作系统命令注入	CNNVD-202101-1151	DELL	DELL Dell EMC Avamar Server 操作系统命令注入漏洞 (CNNVD-202101-1151)
		CNNVD-202101-409	Evolucare	
		CNNVD-202101-087	NEC	
		CNNVD-202101-332	Tp-link	
		CNNVD-202101-2240	个人开发者	
5	缓冲区错误	CNNVD-202101-2482	Accfly	Google Android 缓冲区错误漏洞 (CNNVD-202101-251)
		CNNVD-202101-2484		
		CNNVD-202101-2483		
		CNNVD-202101-2481		
		CNNVD-202101-1535	Cisco	
		CNNVD-202101-1536		
		CNNVD-202101-2549	D-Link	
		CNNVD-202101-1655	Eclipse 基金会	

		CNNVD-202101-358	Fortinet	
		CNNVD-202101-251	Google	
		CNNVD-202101-1046	Huawei	
		CNNVD-202101-1099		
		CNNVD-202101-1049	Huawei,Honor	
		CNNVD-202101-1098		
		CNNVD-202101-502	Live Networks	
		CNNVD-202101-2254	Mozilla 基金会	
		CNNVD-202101-1467	Python 基金会	
		CNNVD-202101-2230	Sagemcom	
		CNNVD-202101-915	Siemens	
		CNNVD-202101-917		
		CNNVD-202101-341	Wolfssl	
6	访问控制错误	CNNVD-202101-2367	Geeni	IBM Security Identity Governance and Intelligence 访问控制错误漏洞 (CNNVD-202101-1633)
		CNNVD-202101-413	Google	
		CNNVD-202101-1472	HGiga	
		CNNVD-202101-1633	IBM	
		CNNVD-202101-250	Red Lion Controls	
7	资源管理错误	CNNVD-202101-419	Google	Google Chrome 资源管理错误漏洞 (CNNVD-202101-390)
		CNNVD-202101-418		
		CNNVD-202101-1137		
		CNNVD-202101-390		
		CNNVD-202101-425		
		CNNVD-202101-414		
		CNNVD-202101-417		
8	输入验证错误	CNNVD-202101-1146	Apache 基金会	WordPress 输入验证错误漏洞(CNNVD-202101-047)
		CNNVD-202101-2039	Caret	
		CNNVD-202101-1524	Cisco	
		CNNVD-202101-1625		
		CNNVD-202101-1061	Git Big Ppicture	
		CNNVD-202101-521	Gogo	
		CNNVD-202101-1291	HPE	
		CNNVD-202101-1041	Huawei,Honor	
		CNNVD-202101-047	Wordpress 基金会	

1. Cisco SD-WAN vManage Software SQL 注入漏洞（CNNVD-202101-1516）

Cisco SD-WAN vManage Software 是美国思科（Cisco）公司的一款用于 SD-WAN（软件定义广域网络）解决方案的管理软件。

Cisco SD-WAN vManage Software 存在 SQL 注入漏洞，该漏洞源于 web 管理界面对 SQL 查询语句验证不严格导致。攻击者可利用该漏洞对应用程序进行身份验证并向受影响的系统发送恶意 SQL 查询。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-sqlinjm-xV8dsjq5

2. Apache Dubbo 代码问题漏洞（CNNVD-202101-520）

Apache Dubbo 是美国阿帕奇软件（Apache）基金会的一款基于 Java 的轻量级 RPC（远程过程调用）框架。该产品提供了基于接口的远程呼叫、容错和负载平衡以及自动服务注册和发现等功能。

Apache Dubbo 2.7.5 及之前版本中存在代码问题漏洞。该漏洞源于使用者使用 Hessian2 作为序列化和反序列化的工具，该工具反序列化 HashMap 对象的时候，同时会执行一些代码从而触发漏洞。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://lists.apache.org/thread.html/r5b2df4ef479209dc4ced457b3d58a887763b60b9354c3dc148b2eb5b%40%3Cdev.dubbo.apache.org%3E

3. Oracle Fusion Middleware WebLogic Server 授权问题漏洞（CNNVD-202101-1343）

Oracle WebLogic Server 是美国甲骨文（Oracle）公司的一款适用

于云环境和传统环境的应用服务中间件，它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。

Oracle Fusion Middleware 的 Oracle WebLogic Server 组件存在授权问题漏洞，该漏洞允许未经身份验证的攻击者通过 IIOP、T3 进行网络访问，从而危及 Oracle WebLogic Server。以下产品及版本受到影响：Oracle WebLogic Server--Core Components--12.1.3.0.0。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

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

4. DELL Dell EMC Avamar Server 操作系统命令注入漏洞（CNNVD-202101-1151）

DELL Dell EMC Avamar Server 是美国戴尔（DELL）公司的一套用于服务器的完全虚拟化的备份和恢复软件。

DELL EMC Avamar Server, versions 19.1, 19.2, 19.3 存在操作系统命令注入漏洞，未经身份验证的远程攻击者，可以在应用程序的底层操作系统上执行任意操作系统命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.dell.com/support/kbdoc/en-us/000181806/dsa-2020-272-dell-emc-avamar-server-security-update-for-multiple-vulnerabilities

5. Google Android 缓冲区错误漏洞（CNNVD-202101-251）

Google Android 是美国谷歌开放手持设备联盟（Google）的一套以 Linux 为基础的开源操作系统。

Google Android OS 存在缓冲区错误漏洞，该漏洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致相关联的其他内存位置上执行了错误的读写操作。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://source.android.com/security/bulletin/2021-01-01

6. IBM Security Identity Governance and Intelligence 访问控制错误漏洞（CNNVD-202101-1633）

IBM Security Identity Governance and Intelligence（IGI）是美国 IBM 公司的一套身份治理解决方案。该产品包括生命周期管理、访问风险评估和身份认证管理等功能。

IBM Security Identity Governance and Intelligence 5.2.6 存在安全漏洞，该漏洞源于程序对于需要验证的用户身份消耗大量资源，导致程序不执行任何身份验证。攻击者可利用该漏洞绕过身份验证。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.ibm.com/support/pages/node/6403247

7. Google Chrome 资源管理错误漏洞（CNNVD-202101-390）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。

Google Chrome 87.0.4280.141 之前版本中存在资源管理错误漏洞，攻击者可利用该漏洞执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2021/01/stable-channel-upda

te-for-desktop.html

8. WordPress 输入验证错误漏洞（CNNVD-202101-047）

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。

Ultimate Member plugin before 2.1.12 for WordPress 存在安全漏洞，该漏洞源于没有在注册过程中提供 role 参数进行过滤，攻击者可利用该漏洞提升特权。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.wordfence.com/blog/2020/11/critical-privilege-escalation-vulnerabilities-affect-100k-sites-using-ultimate-member-plugin/

1.4.2 高危漏洞实例

本月高危漏洞共 659 个，其中重点漏洞实例如表 6 所示。

表 6　2021 年 1 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	SQL 注入	CNNVD-202101-524	Cacti 团队	Microsoft SQL Server SQL 注入漏洞（CNNVD-202101-796）
		CNNVD-202101-1610	Cisco	
		CNNVD-202101-1513		
		CNNVD-202101-1517		
		CNNVD-202101-1470	HGiga	
		CNNVD-202101-2027	Hyweb	
		CNNVD-202101-1592	IBM	
		CNNVD-202101-366	Invision	
		CNNVD-202101-796	Microsoft	
		CNNVD-202101-244	Orangehrm	
		CNNVD-202101-1491	ZOHO	
		CNNVD-202101-533	Zzcms 团队	
		CNNVD-202101-410	个人开发者	
2	代码问题	CNNVD-202101-1321	ASUS	Apache Servicecomb Java Chassis 代码问题漏洞
		CNNVD-202101-939	Adobe	

		CNNVD-202101-942		（CNNVD-202101-2045）
		CNNVD-202101-943		
		CNNVD-202101-936		
		CNNVD-202101-941		
		CNNVD-202101-536	Anydesk	
		CNNVD-202101-2045	Apache 基金会	
		CNNVD-202101-1560	Check Point	
		CNNVD-202101-1537	Cisco	
		CNNVD-202101-1549		
		CNNVD-202101-966		
		CNNVD-202101-967		
		CNNVD-202101-1085	Cloudbees	
		CNNVD-202101-254	Delta Electronics	
		CNNVD-202101-393		
		CNNVD-202101-007	Drupal 社区	
		CNNVD-202101-330	FasterXML	
		CNNVD-202101-329		
		CNNVD-202101-326		
		CNNVD-202101-325		
		CNNVD-202101-337		
		CNNVD-202101-331		
		CNNVD-202101-371		
		CNNVD-202101-344		
		CNNVD-202101-327		
		CNNVD-202101-355		
		CNNVD-202101-1474		
		CNNVD-202101-333		
		CNNVD-202101-2353	Fehi	
		CNNVD-202101-1462	Files.com	
		CNNVD-202101-282	Genivia	
		CNNVD-202101-1302	Git Lfs 团队	
		CNNVD-202101-1290	HPE	
		CNNVD-202101-1636	Honeywell	
		CNNVD-202101-270	IBM	
		CNNVD-202101-2041		
		CNNVD-202101-1106	Juniper Networks	
		CNNVD-202101-1634	M&M	
		CNNVD-202101-2405	Micrium	
		CNNVD-202101-1473	Micro Focus	
		CNNVD-202101-269	NXLog	

		CNNVD-202101-458	Nvidia	
		CNNVD-202101-1538	OpenEMR	
		CNNVD-202101-1514	OpenMage	
		CNNVD-202101-1650	OpenMage 组织	
		CNNVD-202101-348	Proofpoint	
		CNNVD-202101-350		
		CNNVD-202101-243	Red Lion Controls	
		CNNVD-202101-2331	Rostelecom	
		CNNVD-202101-926	Schneider Electric	
		CNNVD-202101-925		
		CNNVD-202101-844	Siemens	
		CNNVD-202101-938	Sky	
		CNNVD-202101-1090	Sound Research	
		CNNVD-202101-907	TIBCO	
		CNNVD-202101-1284	Theonedev	
		CNNVD-202101-296	Veritas	
		CNNVD-202101-1484	个人开发者	
3	授权问题	CNNVD-202101-2471	Apache 基金会	Oracle Fusion Middleware 组件授权问题漏洞（CNNVD-202101-1447）
		CNNVD-202101-1559	Cisco	
		CNNVD-202101-103	Dell	
		CNNVD-202101-1123	Juniper Networks	
		CNNVD-202101-023	Loopring 社区	
		CNNVD-202101-892	Microsoft	
		CNNVD-202101-913		
		CNNVD-202101-890		
		CNNVD-202101-082	NEC	
		CNNVD-202101-1364	Oracle	
		CNNVD-202101-1339		
		CNNVD-202101-1439		
		CNNVD-202101-1366		
		CNNVD-202101-1454		
		CNNVD-202101-1324		
		CNNVD-202101-1349		
		CNNVD-202101-1389		
		CNNVD-202101-1329		
		CNNVD-202101-1359		

		CNNVD-202101-1447		
		CNNVD-202101-1344		
		CNNVD-202101-1451		
		CNNVD-202101-1361		
		CNNVD-202101-1422		
		CNNVD-202101-1334		
		CNNVD-202101-1459		
		CNNVD-202101-1436		
		CNNVD-202101-1457		
		CNNVD-202101-1340		
		CNNVD-202101-1437		
		CNNVD-202101-924	Siemens	
		CNNVD-202101-1125	Xiaomi	
		CNNVD-202101-2561	ZIV	
		CNNVD-202101-523	个人开发者	
		CNNVD-202101-499		
		CNNVD-202101-859	北京坤豆	
4	操作系统命令注入	CNNVD-202101-1554	Cisco	Fortinet FortiDeceptor 操作系统命令注入漏洞（CNNVD-202101-363）
		CNNVD-202101-363	Fortinet	
		CNNVD-202101-1118	Juniper Networks	
		CNNVD-202101-1045	Nagios	
		CNNVD-202101-1066	Pepperl Fuchs	
		CNNVD-202101-1616	Philips	
		CNNVD-202101-532	Smartbear	
		CNNVD-202101-436	Sonicwall	
5	缓冲区错误	CNNVD-202101-945	Adobe	Google Chrome 缓冲区错误漏洞（CNNVD-202101-400）
		CNNVD-202101-944		
		CNNVD-202101-969	Cisco	
		CNNVD-202101-1009		
		CNNVD-202101-1003		
		CNNVD-202101-984		
		CNNVD-202101-976		
		CNNVD-202101-1012		
		CNNVD-202101-1018		
		CNNVD-202101-1076		
		CNNVD-202101-988		
		CNNVD-202101-980		
		CNNVD-202101-971		
		CNNVD-202101-960		
		CNNVD-202101-989		

		CNNVD-202101-1001		
		CNNVD-202101-1013		
		CNNVD-202101-1017		
		CNNVD-202101-1111		
		CNNVD-202101-1007		
		CNNVD-202101-950		
		CNNVD-202101-972		
		CNNVD-202101-1547		
		CNNVD-202101-990		
		CNNVD-202101-1011		
		CNNVD-202101-986		
		CNNVD-202101-1544		
		CNNVD-202101-1002		
		CNNVD-202101-978		
		CNNVD-202101-993		
		CNNVD-202101-999		
		CNNVD-202101-1044		
		CNNVD-202101-998		
		CNNVD-202101-991		
		CNNVD-202101-997		
		CNNVD-202101-992		
		CNNVD-202101-1079		
		CNNVD-202101-982		
		CNNVD-202101-1093		
		CNNVD-202101-1109		
		CNNVD-202101-973		
		CNNVD-202101-1543		
		CNNVD-202101-979		
		CNNVD-202101-985		
		CNNVD-202101-970		
		CNNVD-202101-1006		
		CNNVD-202101-1091		
		CNNVD-202101-1008		
		CNNVD-202101-1021		
		CNNVD-202101-987		
		CNNVD-202101-1092		
		CNNVD-202101-1107		
		CNNVD-202101-1548		
		CNNVD-202101-974		
		CNNVD-202101-963		
		CNNVD-202101-981		
		CNNVD-202101-995		

		CNNVD-202101-1078		
		CNNVD-202101-1620		
		CNNVD-202101-1010		
		CNNVD-202101-996		
		CNNVD-202101-1104		
		CNNVD-202101-977		
		CNNVD-202101-994		
		CNNVD-202101-1005		
		CNNVD-202101-1000		
		CNNVD-202101-983		
		CNNVD-202101-975		
		CNNVD-202101-1463	D-link	
		CNNVD-202101-394	Delta Electronics	
		CNNVD-202101-255		
		CNNVD-202101-258		
		CNNVD-202101-398		
		CNNVD-202101-1641		
		CNNVD-202101-1638		
		CNNVD-202101-401	Eaton	
		CNNVD-202101-666	Espressif	
		CNNVD-202101-028	FFmpeg	
		CNNVD-202101-2398	Fuji Electric	
		CNNVD-202101-2403		
		CNNVD-202101-2406		
		CNNVD-202101-2401		
		CNNVD-202101-2393		
		CNNVD-202101-384	Google	
		CNNVD-202101-213		
		CNNVD-202101-400		
		CNNVD-202101-2361		
		CNNVD-202101-1596		
		CNNVD-202101-2584	HPE	
		CNNVD-202101-2548		
		CNNVD-202101-2550		
		CNNVD-202101-2545		
		CNNVD-202101-2547		
		CNNVD-202101-2570		
		CNNVD-202101-2546		
		CNNVD-202101-2555		
		CNNVD-202101-2543		
		CNNVD-202101-2582		
		CNNVD-202101-2544		

		CNNVD-202101-1639	Honeywell	
		CNNVD-202101-1117	Juniper Networks	
		CNNVD-202101-512	K7 Computing Pvt	
		CNNVD-202101-506		
		CNNVD-202101-507		
		CNNVD-202101-528		
		CNNVD-202101-511		
		CNNVD-202101-792	Microsoft	
		CNNVD-202101-802		
		CNNVD-202101-1508	NVIDIA	
		CNNVD-202101-457		
		CNNVD-202101-408	Omron	
		CNNVD-202101-1314	Open Design Alliance	
		CNNVD-202101-2374	OpenLDAP 基金会	
		CNNVD-202101-236	Panasonic	
		CNNVD-202101-496	Pillow 团队	
		CNNVD-202101-1653	Qualcomm	
		CNNVD-202101-266		
		CNNVD-202101-391	Rockwell Automation	
		CNNVD-202101-776	SAP	
		CNNVD-202101-769		
		CNNVD-202101-775		
		CNNVD-202101-770		
		CNNVD-202101-781		
		CNNVD-202101-777		
		CNNVD-202101-774		
		CNNVD-202101-773		
		CNNVD-202101-779		
		CNNVD-202101-780		
		CNNVD-202101-772		
		CNNVD-202101-771		
		CNNVD-202101-763		
		CNNVD-202101-778		
		CNNVD-202101-765		
		CNNVD-202101-259	Samsung	
		CNNVD-202101-257		
		CNNVD-202101-850	Siemens	
		CNNVD-202101-873		

		CNNVD-202101-920		
		CNNVD-202101-921		
		CNNVD-202101-841		
		CNNVD-202101-843		
		CNNVD-202101-837		
		CNNVD-202101-845		
		CNNVD-202101-838		
		CNNVD-202101-918		
		CNNVD-202101-840		
		CNNVD-202101-849		
		CNNVD-202101-839		
		CNNVD-202101-854		
		CNNVD-202101-848		
		CNNVD-202101-833		
		CNNVD-202101-852		
		CNNVD-202101-851		
		CNNVD-202101-288	Softmaker	
		CNNVD-202101-481	Videolan 组织	
		CNNVD-202101-1570	个人开发者	
		CNNVD-202101-2221		
		CNNVD-202101-020		
		CNNVD-202101-497		
		CNNVD-202101-2315		
		CNNVD-202101-1569		
		CNNVD-202101-2454		
		CNNVD-202101-2314		
		CNNVD-202101-1568		
6	访问控制错误	CNNVD-202101-2542	Apache 基金会	Microsoft Windows 远程桌面模块访问控制错误漏洞（CNNVD-202101-868）
		CNNVD-202101-2475		
		CNNVD-202101-1034	Cisco	
		CNNVD-202101-1280	Docker	
		CNNVD-202101-1056	IBM	
		CNNVD-202101-1477		
		CNNVD-202101-535	K7 Computing Pvt	
		CNNVD-202101-530		
		CNNVD-202101-527		
		CNNVD-202101-824	Microsoft	
		CNNVD-202101-807		
		CNNVD-202101-865		
		CNNVD-202101-868		
		CNNVD-202101-862		

		CNNVD-202101-846		
		CNNVD-202101-2494	Opensolution	
		CNNVD-202101-1345	Oracle	
		CNNVD-202101-1335		
		CNNVD-202101-1427		
		CNNVD-202101-1435		
		CNNVD-202101-1417		
		CNNVD-202101-1369		
		CNNVD-202101-1453		
		CNNVD-202101-2350	Pyres	
		CNNVD-202101-2593	Star Computer	
		CNNVD-202101-2590		
		CNNVD-202101-224	Veritas	
		CNNVD-202101-219		
		CNNVD-202101-227		
		CNNVD-202101-242	Viki Solutions	
		CNNVD-202101-403	个人开发者	
		CNNVD-202101-2344		
		CNNVD-202101-2031		
7	资源管理错误	CNNVD-202101-1528	Cisco	Google Chrome 资源管理错误漏洞（CNNVD-202101-1133）
		CNNVD-202101-1642	Delta Electronics	
		CNNVD-202101-471	GitLab	
		CNNVD-202101-404	Google	
		CNNVD-202101-1580		
		CNNVD-202101-397		
		CNNVD-202101-212		
		CNNVD-202101-231		
		CNNVD-202101-1133		
		CNNVD-202101-216		
		CNNVD-202101-1637	Honeywell	
		CNNVD-202101-1654	IBM	
		CNNVD-202101-290	Joyent	
		CNNVD-202101-1101	Juniper Networks	
		CNNVD-202101-1635	Mitsubishi Electric	
		CNNVD-202101-2286	Nextcloud	
		CNNVD-202101-2033	Openjs 基金会	

		CNNVD-202101-2296	Openldap 基金会	
		CNNVD-202101-782	SAP	
		CNNVD-202101-376	Socketio 社区	
		CNNVD-202101-375		
		CNNVD-202101-2564	ZIV	
		CNNVD-202101-2270	ZTE	
		CNNVD-202101-1048	个人开发者	
8	输入验证错误	CNNVD-202101-1534	Cisco	Cisco SD-WAN vManage Software 输入验证错误漏洞（CNNVD-202101-1534）
		CNNVD-202101-1627		
		CNNVD-202101-1626		
		CNNVD-202101-1084	Cloudbees	
		CNNVD-202101-005	Drupal 社区	
		CNNVD-202101-206	Google	
		CNNVD-202101-018		
		CNNVD-202101-019		
		CNNVD-202101-1110	Juniper Networks	
		CNNVD-202101-2310	Kaspersky	
		CNNVD-202101-2579	Mitel Networks	
		CNNVD-202101-461	Nvidia	
		CNNVD-202101-478		
		CNNVD-202101-479		
		CNNVD-202101-456		
		CNNVD-202101-459		
		CNNVD-202101-2336	Opera Software	
		CNNVD-202101-1075	Owasp 基金会	
		CNNVD-202101-2038	Red Hat	
		CNNVD-202101-2036	Revive Adserver 团队	
		CNNVD-202101-279	个人开发者	
		CNNVD-202101-1499		
		CNNVD-202101-241		
		CNNVD-202101-030		

1. Microsoft SQL Server SQL 注入漏洞（CNNVD-202101-796）

Microsoft SQL Server 是美国微软（Microsoft）公司的一套应用在 Microsoft Windows 系统下的大型商业数据库系统。

Microsoft SQL 存在 SQL 注入漏洞,目前尚无此漏洞的相关信息，请随时关注 CNNVD 或厂商公告。以下产品及版本受到影响:Microsoft SQL Server 2019 for x64-based Systems (GDR),Microsoft SQL Server 2019 for x64-based Systems (CU 8),Microsoft SQL Server 2016 Service Pack 2 for x64-based Systems (CU 15),Microsoft SQL Server 2017 for x64-based Systems (CU 22),Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4),Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU 4),Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR),Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (GDR), Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR),Microsoft SQL Server 2017 for x64-based Systems (GDR),Microsoft SQL Server 2012 for x64-based Systems Service Pack 4 (QFE),Microsoft SQL Server 2012 for 32-bit Systems Service Pack 4 (QFE)。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1636

2. Apache Servicecomb Java Chassis 代码问题漏洞

（CNNVD-202101-2045）

Apache Servicecomb Java Chassis 是 Apache 基金会的一个基于 Java 语言用于为构建微服务提供整个解决方案的代码库。

Apache ServiceComb-Java-Chassis 2.1.5 之前版本存在代码问题漏洞，该漏洞允许经过身份验证的用户注入一些数据并导致任意代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://issues.apache.org/jira/browse/SCB-2145

3. Oracle Fusion Middleware 组件授权问题漏洞

（CNNVD-202101-1447）

Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。Outside In Technology 是其中的一个软件开发工具包组件。

Oracle Fusion Middleware 的 Oracle Outside In Technology 组件存在授权问题漏洞，该漏洞允许未经身份验证的攻击者通过 HTTP 进行网络访问，从而在技术上破坏 Oracle。以下产品及版本受到影响：Oracle Outside In Technology--Outside In Filters--8.5.4, 8.5.5。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

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

4. Fortinet FortiDeceptor 操作系统命令注入漏洞

（CNNVD-202101-363）

Fortinet FortiDeceptor 是美国飞塔（Fortinet）公司的一款网络威

胁检测平台。该平台主要通过欺骗技术暴露网络威胁等。

FortiDeceptor 3.0.0, 3.0.1, 3.1.0 存在安全漏洞，该漏洞允许远程用户在目标系统上执行任意 shell 命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.fortiguard.com/psirt/FG-IR-20-177

5. Google Chrome 缓冲区错误漏洞（CNNVD-202101-400）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。

Google Chrome 87.0.4280.141 之前版本中存在缓冲区错误漏洞，攻击者可利用该漏洞执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html

6. Microsoft Windows 远程桌面模块访问控制错误漏洞（CNNVD-202101-868）

Microsoft Windows 是美国微软（Microsoft）公司的一套个人设备使用的操作系统。

Microsoft Windows 远程桌面模块访问控制错误漏洞,目前尚无此漏洞的相关信息，请随时关注 CNNVD 或厂商公告。以下产品及版本受到影响:Windows 10 Version 1909 for ARM64-based Systems, Windows 10 Version 1909 for x64-based Systems,Windows 10 Version 1909 for 32-bit Systems,Windows Server 2019 (Server Core installation),Windows Server 2019,Windows 10 Version 1809 for ARM

64-based Systems,Windows 10 Version 1809 for x64-based Systems, Windows 10 Version 1809 for 32-bit Systems,Windows 10 Version 1803 for ARM64-based Systems,Windows 10 Version 1803 for x64-based Systems,Windows 10 Version 1803 for 32-bit Systems,Windows Server, version 20H2 (Server Core Installation),Windows 10 Version 20H2 for ARM64-based Systems,Windows 10 Version 20H2 for 32-bit Systems,Windows 10 Version 20H2 for x64-based Systems, Windows Server 2012 R2 (Server Core installation),Windows Server 2012 R2 (Server Core installation),Windows Server 2012 R2,Windows Server 2012 R2,Windows Server 2012 (Server Core installation), Windows Server 2012 (Server Core installation),Windows Server 2012,Windows Server 2012,Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation),Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation),Windows Server 2008 R2 for x64-based Systems Service Pack 1,Windows Server 2008 R2 for x64-based Systems Service Pack 1, Windows RT 8.1,Windows 8.1 for x64-based systems,Windows 8.1 for x64-based systems,Windows 8.1 for 32-bit systems,Windows 8.1 for 32-bit systems,Windows 7 for x64-based Systems Service Pack 1,Windows 7 for x64-based Systems Service Pack 1,Windows 7 for 32-bit Systems Service Pack 1,Windows 7 for 32-bit Systems Service Pack 1,Windows Server 2016 (Server Core installation),Window

s Server 2016,Windows 10 Version 1607 for x64-based Systems,Windows 10 Version 1607 for 32-bit Systems,Windows 10 for x64-based Systems,Windows 10 for 32-bit Systems,Windows Server, version 2004 (Server Core installation),Windows 10 Version 2004 for x64-based Systems,Windows 10 Version 2004 for ARM64-based Systems, Windows 10 Version 2004 for 32-bit Systems,Windows Server, version 1909 (Server Core installation)。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1674

7. Google Chrome 资源管理错误漏洞（CNNVD-202101-1133）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。

Google Chrome prior to 81.0.4044.92 存在资源管理错误漏洞，该漏洞允许远程攻击者执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2020/04/stable-channel-update-for-desktop_7.html

8. Cisco SD-WAN vManage Software 输入验证错误漏洞（CNNVD-202101-1534）

Cisco SD-WAN vManage Software 是美国思科（Cisco）公司的一款用于 SD-WAN（软件定义广域网络）解决方案的管理软件。

Cisco SD-WAN vManage Software 的 web-based management i

nterface 存在输入验证错误漏洞，该漏洞允许经过身份验证的远程攻击者可利用该漏洞绕过授权，修改受影响系统的配置，访问敏感信息，并查看他们未被授权访问的信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS

二、接报漏洞情况

本月接报漏洞 12693 个，其中信息技术产品漏洞（通用型漏洞）646 个，网络信息系统漏洞（事件型漏洞）12047 个。

表 7 2021 年 1 月漏洞接报情况

序号	报送单位	漏洞总量
1	上海斗象信息科技有限公司	6136
2	网神信息技术（北京）股份有限公司	3604
3	北京山石网科信息技术有限公司	697
4	北京数字观星科技有限公司	505
5	北京华云安信息技术有限公司	327
6	山东华鲁科技发展股份有限公司	201
7	北京天地和兴科技有限公司	174
8	北京安信天行科技有限公司	118
9	山东新潮信息技术有限公司	88
10	深圳开源互联网安全技术有限公司	88
11	河南听潮盛世信息技术有限公司	68

12	北京启明星辰信息安全技术有限公司	67
13	西安四叶草信息技术有限公司	60
14	西安交大捷普网络科技有限公司	49
15	北京顶象技术有限公司	44
16	华为技术有限公司未然实验室	39
17	安徽长泰信息安全服务有限公司	34
18	山东云天安全技术有限公司	27
19	北京圣博润高新技术股份有限公司	26
20	杭州海康威视数字技术股份有限公司	23
21	北京时代新威信息技术有限公司	20
22	广州锦行网络科技有限公司	20
23	星云博创摘星实验室	20
24	湖南匡安网络技术有限公司	20
25	恒安嘉新(北京)科技股份公司	19
26	上海安识网络科技有限公司	18
27	中国电信集团系统集成有限责任公司	14
28	广州竞远安全技术股份有限公司	13
29	上海安洵信息技术有限公司	11
30	杭州安恒信息技术股份有限公司	11
31	杭州默安科技有限公司	11
32	北京赋云安运营科技有限公司	10
33	博智安全科技股份有限公司	10
34	安徽华云网安信息技术有限公司	10

35	深信服科技股份有限公司	10
36	远江盛邦（北京）网络安全科技股份有限公司	10
37	浪潮电子信息产业股份有限公司	9
38	亚信科技（成都）有限公司	8
39	中电长城网际系统应用有限公司	7
40	四川虹微技术有限公司	6
41	中兴通讯股份有限公司	5
42	中国科学院软件研究所	5
43	北京云测信息技术有限公司	5
44	北京智游网安科技有限公司	5
45	北京网御星云信息技术有限公司	4
46	广东网安科技有限公司	4
47	浙江宇视科技有限公司	4
48	个人	3
49	北京天融信网络安全技术有限公司	3
50	安全邦（北京）信息技术有限公司	3
51	西北工业大学网络空间安全学院	3
52	博智安全科技股份有限公司	2
53	任子行信息技术有限公司	2
54	北京威努特技术有限公司	2
55	中国信息安全测评中心华中测评中心	1
56	北京天融信网络安全技术有限公司	1
57	北京安华金和科技有限公司	1

58	北京安帝科技有限公司	1
59	北京市星阑科技有限公司	1
60	北京江南天安科技有限公司	1
61	嘀嗒出行	1
62	国防科技大学	1
63	海南神州希望网络有限公司	1
64	腾讯安全天马实验室	1
65	长扬科技(北京)有限公司	1
报送总计		12693

三、重大漏洞预警

3.1 SonicWall SSL-VPN 安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 SonicWall SSL-VPN 安全漏洞（CNNVD-202101-2409）情况的报送。成功利用漏洞的攻击者可以在未授权的情况下实现远程代码执行，进而控制目标设备。Sonic SMA 8.0.0.4 之前的版本均受漏洞影响。目前，SonicWall 官方已发布版本更新修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

. 漏洞介绍

SonicWall 是硬件防火墙设备、VPN 网关和网络安全解决方案的制造商，SonicWall SSL-VPN 是 SonicWALL 的一款 Vpn 连接方案，该产品应用于远程安全连接。

漏洞源于 Sonicwall SSL-VPN 引入旧版本的 Linux 内核，导致攻击者可以构造恶意的 http 请求注入系统命令，成功利用漏洞的攻击者可以在受影响设备获得 nobody 用户权限并执行任意命令，最终完全控制目标设备。

. 危害影响

成功利用漏洞的攻击者可以在未授权的情况下实现远程代码执行，进而控制目标设备。Sonic SMA 8.0.0.4 之前的版本均受漏洞影响。

. 修复建议

目前，SonicWall 官方已发布版本更新修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

https://www.sonicwall.com/

3.2 致远 OA 文件上传漏洞的预警

近日，国家信息安全漏洞库新增中国用友致远软件技术有限公司的致远 OA 文件上传漏洞 1 个（CNNVD-202101-1460）。成功利用漏洞的攻击者可以在未授权的情况下实现恶意文件上传，从而控制服务器。致远 OA V8.0、V8.0SP1、V7.1、V7.1SP1、V7.0、V7.0SP1、V7.0SP2、

V7.0SP3、V6.0、V6.1SP1、V6.1SP2 版本均受漏洞影响。目前，致远官方已发布版本更新修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

.漏洞介绍

致远 OA 是中国用友致远软件技术有限公司下属的全资子公司北京致远互联软件股份有限公司的一套办公自动化软件。

该漏洞源于致远 OA 部分版本 ajax 接口存在未授权访问，攻击者通过构造恶意请求，可在无需登录的情况下上传恶意文件，从而控制目标服务器。

.危害影响

成功利用漏洞的攻击者可以在未授权的情况下实现恶意文件上传，从而控制服务器。

.修复建议

目前，致远官方已发布版本更新修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

http://service.seeyon.com/patchtools/tp.html#/patchList?type=%E5%AE%89%E5%85%A8%E8%A1%A5%E4%B8%81&id=1