北京师范大学网络信息安全通告

2021 年 8 月报告

北京师范大学信息网络中心

2021 年 9 月

目录

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，2021 年 8 月份新增安全漏洞共 1911 个，从厂商分布来看，WordPress 基金会公司产品的漏洞数量最多，共发布 148 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 15.49%。本月新增漏洞中，超危漏洞 222 个、高危漏洞 760 个、中危漏洞 885 个、低危漏洞 44 个，相应修复率分别为 81.53%、83.95%、87.80%以及 84.09%。合计 1633 个漏洞已有修复补丁发布，本月整体修复率 85.45%。

截至 2021 年 08 月 31 日，CNNVD 采集漏洞总量已达 167566 个。

1.1 漏洞增长概况

2021 年 8 月新增安全漏洞 1911 个，与上月（1827 个）相比增加了 4.60%。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 1716 个。

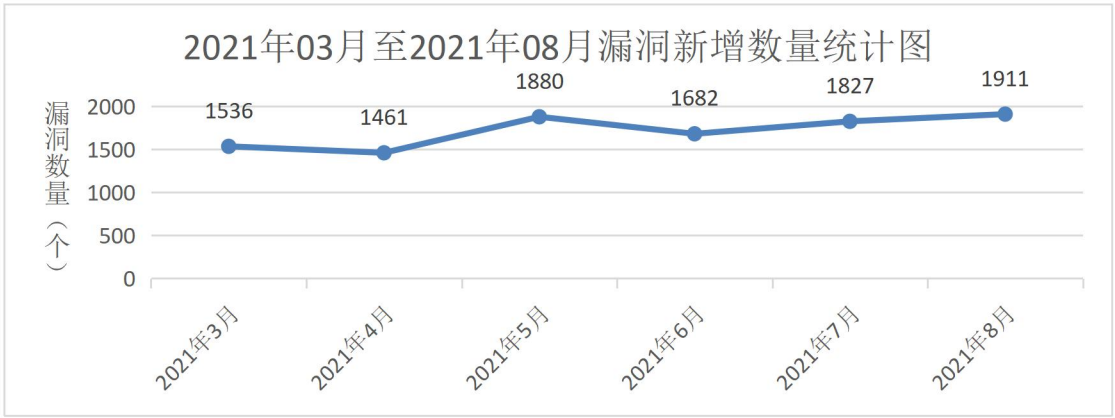

图 1 2021 年 3 月至 8 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

2021 年 8 月厂商漏洞数量分布情况如表 1 所示，WordPress 基金会公司漏洞达到 148 个，占本月漏洞总量的 7.74%。

表 1　2021 年 8 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（个）	所占比例
1	WordPress 基金会	148	7.74%
2	Google	101	5.29%
3	Mozilla 基金会	66	3.45%
4	Microsoft	52	2.72%
5	Huawei	37	1.94%
6	Adobe	35	1.83%
7	F5	31	1.62%
8	NETGEAR	29	1.52%
9	Cisco	28	1.47%
10	IBM	26	1.36%

1.2.2 漏洞产品分布

8 月主流操作系统的漏洞统计情况如表 2 所示。本月 Windows 系列操作系统漏洞数量共 30 个，Windows Server 2019 漏洞数量最多，共 25 个，占主流操作系统漏洞总量的 12.44%，排名第一。

表 2　2021 年 8 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 Server 2019	25
2	Windows 10	25
3	Windows Server 2016	23
4	Windows Server 2012	19
5	Windows Server 2012 R2	19
6	Windows 8.1	18
7	Windows Rt 8.1	18
8	Linux Kernel	15
9	Windows Server 2008	13

10	Windows Server 2008 R2	13
11	Windows 7	12
12	Android	1

1.2.3 漏洞类型分布

2021 年 8 月份发布的漏洞类型分布如表 3 所示，其中跨站脚本类漏洞所占比例最大，约为 15.49%。

表 3 2021 年 8 月漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	跨站脚本	296	15.49%
2	缓冲区错误	180	9.42%
3	代码问题	146	7.64%
4	输入验证错误	142	7.43%
5	SQL 注入	82	4.29%
6	授权问题	55	2.88%
7	资源管理错误	52	2.72%
8	跨站请求伪造	50	2.62%
9	信息泄露	49	2.56%
10	命令注入	46	2.41%
11	代码注入	45	2.35%
12	路径遍历	39	2.04%
13	访问控制错误	36	1.88%
14	权限许可和访问控制问题	35	1.83%
15	信任管理问题	25	1.31%
16	操作系统命令注入	25	1.31%
17	数字错误	22	1.15%
18	注入	19	0.99%
19	安全特征问题	13	0.68%
20	加密问题	10	0.52%
21	数据伪造问题	9	0.47%
22	处理逻辑错误	8	0.42%
23	竞争条件问题	8	0.42%
24	日志信息泄露	5	0.26%
25	后置链接	5	0.26%
26	环境问题	4	0.21%
27	参数注入	3	0.16%
28	配置错误	2	0.10%
29	格式化字符串错误	1	0.05%
30	默认配置问题	1	0.05%

31	调试信息泄露	0	0.00%
32	其他	498	26.06%

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。2021 年 8 月漏洞危害等级分布如图 2 所示，其中超危漏洞 222 条，占本月漏洞总数的 11.62%。

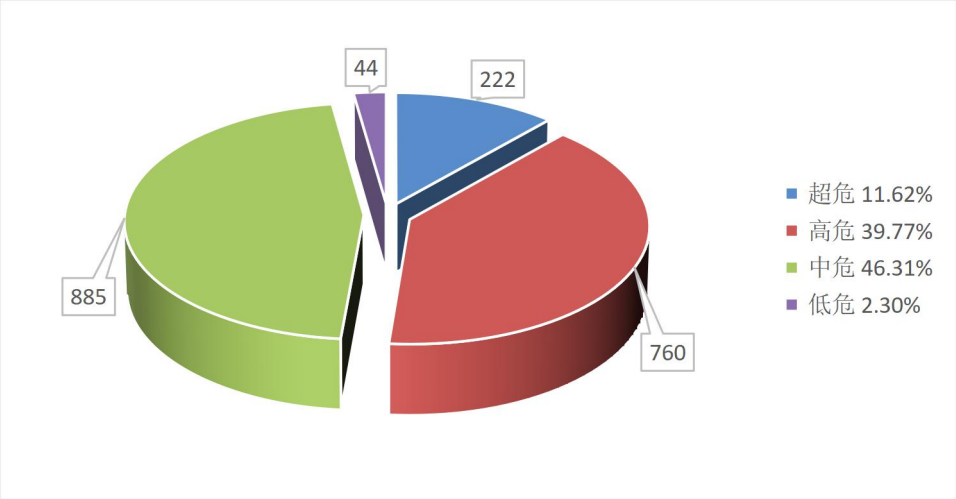

图 2　2021 年 8 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1　整体修复情况

2021 年 8 月漏洞修复情况按危害等级进行统计见图 3。其中中危漏洞修复率最高，达到 87.80%，超危漏洞修复率最低，比例为 81.53%。

总体来看，本月整体修复率，由上月的 88.29%下降至本月的 85.45%。

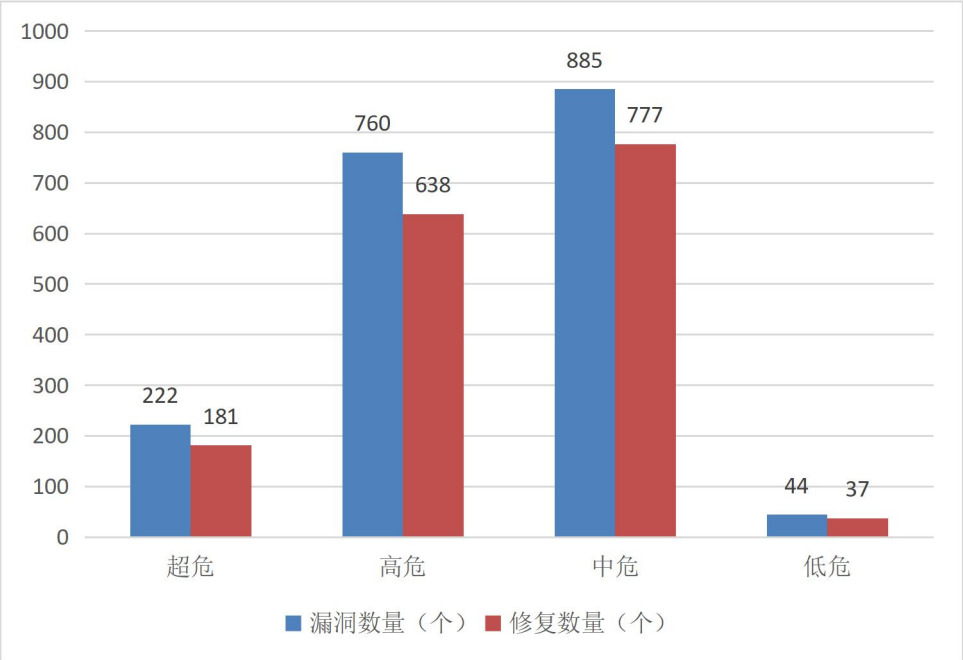

图 3　2021 年 8 月漏洞修复数量统计

1.3.2　厂商修复情况

2021 年 8 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 WordPress 基金会、Google、Mozilla 基金会等十个厂商共 553 条漏洞，占本月漏洞总数的 28.94%，漏洞修复率为 94.94%，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 Microsoft、Huawei、Adobe、NETGEAR、Cisco、IBM 等公司本月漏洞修复率均为 100%，共 525 条漏洞已全部修复。

表 4　2021 年 8 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	WordPress 基金会	148	145	97.97%
2	Google	101	96	95.05%
3	Mozilla 基金会	66	56	84.85%
4	Microsoft	52	52	100.00%
5	Huawei	37	37	100.00%
6	Adobe	35	35	100.00%
7	F5	31	21	67.74%
8	NETGEAR	29	29	100.00%
9	Cisco	28	28	100.00%

10	IBM	26	26	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 222 个，其中重要漏洞实例如表 5 所示。

表 5　2021 年 8 月超危漏洞实例

漏洞类型	厂商	CNNVD编号	漏洞实例
SQL注入	Centreon	CNNVD-202108-312	Fortinet FortiPortal SQL注入漏洞（CNNVD-202108-275）
	Claroty	CNNVD-202108-422	
	Delta Electronics	CNNVD-202108-2397	
		CNNVD-202108-2403	
		CNNVD-202108-2404	
		CNNVD-202108-2406	
	Fortinet	CNNVD-202108-275	
	Foxit	CNNVD-202108-1131	
	Gxlcms	CNNVD-202108-1169	
	Nagios	CNNVD-202108-1357	
	Nuance Communications	CNNVD-202108-1208	
	PrestaShop	CNNVD-202108-1936	
	Progress Software	CNNVD-202108-701	
	TYPO3	CNNVD-202108-914	
		CNNVD-202108-969	
	WordPress基金会	CNNVD-202108-777	
		CNNVD-202108-1863	
	个人开发者	CNNVD-202108-282	
		CNNVD-202108-664	
		CNNVD-202108-704	
		CNNVD-202108-1239	
		CNNVD-202108-1434	
		CNNVD-202108-1593	
		CNNVD-202108-1634	
		CNNVD-202108-1685	
		CNNVD-202108-1938	
		CNNVD-202108-2419	
代码问题	Altova	CNNVD-202108-1054	ZOHO ManageEngine Log360 代码问题漏洞（CNNVD-202108-2670）
	Apache基金会	CNNVD-202108-1150	
	Delta Electronics	CNNVD-202108-2407	
	DevExpress	CNNVD-202108-399	
	Django基金会	CNNVD-202108-1435	
	HCL	CNNVD-202108-1389	
	Jetbrains	CNNVD-202108-656	

	Nagios	CNNVD-202108-1362	
	Nature Easy Soft Network Technology	CNNVD-202108-471	
	Neo4j	CNNVD-202108-494	
	ON24	CNNVD-202108-1390	
	SourceCodester	CNNVD-202108-330	
		CNNVD-202108-331	
	Swisslog Healthcare	CNNVD-202108-081	
	WordPress基金会	CNNVD-202108-049	
		CNNVD-202108-782	
	ZOHO	CNNVD-202108-2670	
	个人开发者	CNNVD-202108-369	
		CNNVD-202108-694	
		CNNVD-202108-1086	
		CNNVD-202108-1110	
		CNNVD-202108-1163	
		CNNVD-202108-1233	
		CNNVD-202108-1433	
		CNNVD-202108-1436	
		CNNVD-202108-1447	
		CNNVD-202108-1826	
		CNNVD-202108-1935	
授权问题	JetBrains	CNNVD-202108-669	Netgear RBR750 授权问题漏洞（CNNVD-202108-963）
	Microsoft	CNNVD-202108-1396	
	Mitel	CNNVD-202108-1377	
	NetModule	CNNVD-202108-1825	
	Netgear	CNNVD-202108-963	
	Totolink	CNNVD-202108-532	
	WordPress基金会	CNNVD-202108-1693	
		CNNVD-202108-2719	
	Wordpress基金会	CNNVD-202108-1423	
操作系统命令注入	Apache基金会	CNNVD-202108-1930	Realtek Jungle SDK 操作系统命令注入漏洞（CNNVD-202108-1421）
	Cisco	CNNVD-202108-378	
	Nagios	CNNVD-202108-1355	
		CNNVD-202108-1356	
	Tecknodreams	CNNVD-202108-1114	
	个人开发者	CNNVD-202108-1421	
缓冲区错误	3S-Smart Software Solutions	CNNVD-202108-303	Rust 缓冲区错误漏洞（CNNVD-202108-757）
	AT&T Labs实验室	CNNVD-202108-1010	
		CNNVD-202108-1032	
		CNNVD-202108-1044	
		CNNVD-202108-1051	
		CNNVD-202108-1156	
	Advantech	CNNVD-202108-456	
	Disc Soft Ltd	CNNVD-202108-1596	
	Foxit	CNNVD-202108-1107	

		CNNVD-202108-1123	
		CNNVD-202108-1127	
	HCC Embedded	CNNVD-202108-386	
		CNNVD-202108-493	
	Huawei	CNNVD-202108-108	
		CNNVD-202108-126	
	Microsoft	CNNVD-202108-856	
	Mozilla基金会	CNNVD-202108-757	
	Swisslog Healthcare	CNNVD-202108-085	
	个人开发者	CNNVD-202108-284	
		CNNVD-202108-396	
		CNNVD-202108-1088	
		CNNVD-202108-1454	
		CNNVD-202108-1509	
		CNNVD-202108-1945	
访问控制错误	Atlassian	CNNVD-202108-136	Atlassian Jira 访问控制错误漏洞（CNNVD-202108-136）
	Cisco	CNNVD-202108-2357	
	Mitsubishi Electric	CNNVD-202108-679	
	Tecknodreams	CNNVD-202108-1122	
	个人开发者	CNNVD-202108-1440	
		CNNVD-202108-1943	
资源管理错误	Mozilla基金会	CNNVD-202108-711	Rust资源管理错误漏洞（CNNVD-202108-711）
	个人开发者	CNNVD-202108-1005	
输入验证错误	Blackberry	CNNVD-202108-1569	Cisco Small Business 输入验证错误漏洞（CNNVD-202108-1644）
	Cisco	CNNVD-202108-1644	
	Foxit	CNNVD-202108-1121	
	Huawei	CNNVD-202108-105	
		CNNVD-202108-127	
	PACKET TIDE	CNNVD-202108-1207	
	ZOHO	CNNVD-202108-2667	
	个人开发者	CNNVD-202108-1142	
		CNNVD-202108-2809	

1. Fortinet FortiPortal SQL 注入漏洞（CNNVD-202108-275）

Fortinet FortiPortal 是美国飞塔（Fortinet）公司的 FortiGate、FortiWiFi 和 FortiAP 产品线的高级、功能丰富的托管安全分析和管理支持工具，可作为虚拟机供 MSP 使用。

Fortinet FortiPortal 存在 SQL 注入漏洞，该漏洞源于该产品对用户提供的数据没有进行充分的清理。攻击者可利用该漏洞向受影响的应用程序发送专门设计的 HTTP 请求，并在应用程序数据库中执行任

意 SQL 命令。

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://www.cybersecurity-help.cz/vdb/SB2021080312

2. ZOHO ManageEngine Log360 代码问题漏洞（CNNVD-202108-2670）

ZOHO ManageEngine Log360 是美国卓豪（ZOHO）公司的一个集成的日志管理和 Active Directory 审计和警报解决方案。该解决方案可帮助您减轻安全威胁、发现持续的攻击企图、检测可疑的用户活动并遵守监管要求。

ZOHO ManageEngine Log360 中存在代码问题漏洞，该漏洞源于产品允许通过 BCP 文件覆盖系统路径。攻击者可通过该漏洞远程执行代码。以下产品及版本受到影响：Zoho ManageEngine Log360 Build 5225 之前版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.manageengine.com/log-management/9182736/ManageEngine_Log360_64bit.exe

3. Netgear RBR750 授权问题漏洞（CNNVD-202108-963）

Netgear RBR750 是美国网件（Netgear）公司的一套家庭 WiFi 系统。

Netgear RBR750 存在授权问题漏洞，该漏洞源于产品未正确限制来自非授权角色的访问。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://kb.netgear.com/000063777/Security-Advisory-for-Authentication-Bypass-on-Some-Extenders-and-WiFi-Systems-PSV-2020-0008

4. Realtek Jungle SDK 操作系统命令注入漏洞（CNNVD-202108-1421）

Realtek Jungle SDK 是提供了一个 HTTP Web 服务器，公开了一

个管理接口，可用于配置接入点。

Realtek Jungle SDK 2.x 版本至 3.4.14B 版本存在安全漏洞，该漏洞源于软件提供了一个称为'MP Daemon'的诊断工具，其通常编译为'UDPServer'二进制文件。该二进制文件受到多个内存破坏漏洞和任意命令注入漏洞的影响，这些漏洞可被远程未经身份验证的攻击者利用。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf

5. Rust 缓冲区错误漏洞（CNNVD-202108-757）

Rust 是 Mozilla 基金会的一款通用、编译型编程语言。

Rust 0.27.1 之前的 nalgebra crate 中存在安全漏洞，该漏洞源于 nalgebra crate 不能确保元素数等于行数和列数的乘积。该漏洞允许越界内存访问。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://rustsec.org/advisories/RUSTSEC-2021-0070.html

6. Atlassian Jira 访问控制错误漏洞（CNNVD-202108-136）

Atlassian Jira 是澳大利亚 Atlassian 公司的一套缺陷跟踪管理系统。该系统主要用于对工作中各类问题、缺陷进行跟踪管理。

Atlassian Jira 存在安全漏洞，该漏洞允许远程攻击者可利用该漏洞在只知道用户名(即不提供其他身份验证)的情况下登录到用户帐户。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://wiki.resolution.de/doc/saml-sso/5.0.x/all/security-advisories/2021-07-29-authentication-bypass-network-attacker-can-login-to-users-accounts-when-usernames-are-known

7. Rust 资源管理错误漏洞（CNNVD-202108-711）

Rust 是 Mozilla 基金会的一款通用、编译型编程语言。

Rust 中存在安全漏洞。详细信息请关注厂商主页。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://rustsec.org/advisories/RUSTSEC-2020-0100.html

8. Cisco Small Business 输入验证错误漏洞（CNNVD-202108-1644）

Cisco Small Business 是美国思科（Cisco）公司的一个交换机。

Cisco Small Business RV110W、RV130、RV130W 和 RV215W 路由器存在输入验证错误漏洞，该漏洞源于对传入 UPnP 流量的验证不当造成的。该漏洞可能允许未经身份验证的远程攻击者执行任意代码或导致受影响的设备意外重启，从而导致拒绝服务 (DoS) 。

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-cisco-sb-rv-overflow-htpymMB5

1.4.2 高危漏洞实例

本月高危漏洞共 760 个，其中重点漏洞实例如表 6 所示。

表 6 2021 年 8 月高危漏洞实例

漏洞类型	厂商	CNNVD编号	漏洞实例
SQL注入	Centreon	CNNVD-202108-307	Fortinet FortiSandbox SQL注入漏洞（CNNVD-202108-299）
		CNNVD-202108-309	
	Fortinet	CNNVD-202108-299	
	Ljcms	CNNVD-202108-1652	
	Metinfo	CNNVD-202108-1185	
	Naviwebs	CNNVD-202108-678	
	Prestashop	CNNVD-202108-1813	
	Progress Software	CNNVD-202108-501	
	Rukovoditel团队	CNNVD-202108-1591	
		CNNVD-202108-1592	
	WordPress基金会	CNNVD-202108-039	
		CNNVD-202108-040	
		CNNVD-202108-041	
		CNNVD-202108-042	

		CNNVD-202108-043
		CNNVD-202108-045
		CNNVD-202108-046
		CNNVD-202108-055
		CNNVD-202108-063
		CNNVD-202108-064
		CNNVD-202108-096
		CNNVD-202108-786
		CNNVD-202108-799
		CNNVD-202108-1853
		CNNVD-202108-1854
		CNNVD-202108-1860
		CNNVD-202108-1861
		CNNVD-202108-1864
		CNNVD-202108-1865
		CNNVD-202108-1867
		CNNVD-202108-1868
	Wuzhi	CNNVD-202108-1809
	个人开发者	CNNVD-202108-692
		CNNVD-202108-705
		CNNVD-202108-829
		CNNVD-202108-830
		CNNVD-202108-1623
		CNNVD-202108-1941
		CNNVD-202108-1942
		CNNVD-202108-2400
		CNNVD-202108-2401
		CNNVD-202108-2417
代码问题	3S-Smart Software Solutions	CNNVD-202108-406
		CNNVD-202108-408
	Acronis	CNNVD-202108-482
	Aveva	CNNVD-202108-1664
		CNNVD-202108-1665
		CNNVD-202108-1667
		CNNVD-202108-1668
	Cisco	CNNVD-202108-379
	Cognex	CNNVD-202108-1271
	Cpanel	CNNVD-202108-1137
		CNNVD-202108-1140
	D-Link	CNNVD-202108-997
		CNNVD-202108-998
		CNNVD-202108-999
		CNNVD-202108-1023
		CNNVD-202108-1024
		CNNVD-202108-1027
	Ecobee	CNNVD-202108-289

Google TensorFlow 代码问题漏洞（CNNVD-202108-1260）

F5	CNNVD-202108-2290
Fortinet	CNNVD-202108-335
Foxit	CNNVD-202108-1128
Google	CNNVD-202108-1198
	CNNVD-202108-1200
	CNNVD-202108-1201
	CNNVD-202108-1220
	CNNVD-202108-1236
	CNNVD-202108-1245
	CNNVD-202108-1260
	CNNVD-202108-1261
Huawei	CNNVD-202108-133
Intel	CNNVD-202108-1070
	CNNVD-202108-1081
Jenkins	CNNVD-202108-2744
	CNNVD-202108-2747
Lenovo	CNNVD-202108-1583
Liferay	CNNVD-202108-341
Mojang	CNNVD-202108-537
Mulesoft	CNNVD-202108-508
Nextcloud	CNNVD-202108-1663
OGC	CNNVD-202108-1845
Perl	CNNVD-202108-807
Pulse Secure	CNNVD-202108-449
Rundeck	CNNVD-202108-2730
SAP	CNNVD-202108-882
	CNNVD-202108-893
	CNNVD-202108-902
Shopware	CNNVD-202108-1502
Sitecore	CNNVD-202108-1225
TIETEN	CNNVD-202108-1165
Trendnet	CNNVD-202108-1012
	CNNVD-202108-1014
	CNNVD-202108-1015
	CNNVD-202108-1016
	CNNVD-202108-1021
Vmware	CNNVD-202108-528
WordPress基金会	CNNVD-202108-530
	CNNVD-202108-2683
XStream团队	CNNVD-202108-1885
	CNNVD-202108-1886
	CNNVD-202108-1887
	CNNVD-202108-1888
	CNNVD-202108-1890
	CNNVD-202108-1894
	CNNVD-202108-1895

		CNNVD-202108-1896	
		CNNVD-202108-1897	
		CNNVD-202108-1898	
		CNNVD-202108-1899	
		CNNVD-202108-1901	
		CNNVD-202108-1902	
	个人开发者	CNNVD-202108-377	
		CNNVD-202108-536	
		CNNVD-202108-833	
		CNNVD-202108-1109	
		CNNVD-202108-1172	
		CNNVD-202108-1193	
		CNNVD-202108-1387	
		CNNVD-202108-1604	
		CNNVD-202108-1605	
		CNNVD-202108-1820	
		CNNVD-202108-1827	
		CNNVD-202108-1911	
授权问题	Acronis	CNNVD-202108-487	多款Qualcomm产品授权问题漏洞（CNNVD-202108-067）
	Corero Network Security	CNNVD-202108-671	
	Gestionaleamica	CNNVD-202108-685	
	JetBrains	CNNVD-202108-658	
	Liferay	CNNVD-202108-338	
	MONITORAPP	CNNVD-202108-1186	
	Microsoft	CNNVD-202108-877	
	Netgear	CNNVD-202108-2714	
	Nvidia	CNNVD-202108-447	
	Octobercms	CNNVD-202108-2380	
	ProLink	CNNVD-202108-657	
	Qualcomm	CNNVD-202108-062	
		CNNVD-202108-067	
	Siemens	CNNVD-202108-878	
	Swisslog Healthcare	CNNVD-202108-087	
	个人开发者	CNNVD-202108-927	
		CNNVD-202108-1572	
		CNNVD-202108-1573	
		CNNVD-202108-2384	
		CNNVD-202108-2418	
		CNNVD-202108-2738	
		CNNVD-202108-2812	
操作系统命令注入	Altus Sistemas de Automacao	CNNVD-202108-1846	Palo Alto Networks PAN-OS 操作系统命令注入漏洞（CNNVD-202108-1089）
	Centreon	CNNVD-202108-1662	
	D-Link	CNNVD-202108-1456	
	Fortinet	CNNVD-202108-319	
		CNNVD-202108-339	
	Palo Alto Networks	CNNVD-202108-1089	

	Siemens	CNNVD-202108-970	
	个人开发者	CNNVD-202108-291	
		CNNVD-202108-292	
		CNNVD-202108-932	
		CNNVD-202108-934	
		CNNVD-202108-1404	
		CNNVD-202108-1485	
缓冲区错误	AT&T Labs实验室	CNNVD-202108-1151	F5 BIG-IP 缓冲区错误漏洞 （CNNVD-202108-2295）
		CNNVD-202108-1152	
		CNNVD-202108-1154	
	Adobe	CNNVD-202108-1542	
		CNNVD-202108-1550	
		CNNVD-202108-1551	
		CNNVD-202108-1552	
	Apache基金会	CNNVD-202108-1852	
	Aruba Networks	CNNVD-202108-2819	
	Aveva	CNNVD-202108-1666	
	Corel	CNNVD-202108-296	
	Delta Electronics	CNNVD-202108-2379	
	Dut计算机控制工程公司	CNNVD-202108-1384	
	Eclipse基金会	CNNVD-202108-1912	
		CNNVD-202108-1913	
	Ecobee	CNNVD-202108-290	
	Ethereum社区	CNNVD-202108-1946	
	F5	CNNVD-202108-2295	
	FATEK	CNNVD-202108-460	
		CNNVD-202108-479	
		CNNVD-202108-490	
	Fortinet	CNNVD-202108-329	
	Freebsd基金会	CNNVD-202108-2322	
	Google	CNNVD-202108-080	
		CNNVD-202108-088	
		CNNVD-202108-104	
		CNNVD-202108-264	
		CNNVD-202108-265	
		CNNVD-202108-266	
		CNNVD-202108-1209	
		CNNVD-202108-1210	
		CNNVD-202108-1212	
		CNNVD-202108-1214	
		CNNVD-202108-1215	
		CNNVD-202108-1216	
		CNNVD-202108-1217	
		CNNVD-202108-1218	
		CNNVD-202108-1219	
		CNNVD-202108-1222	

	CNNVD-202108-1223
	CNNVD-202108-1238
	CNNVD-202108-1240
	CNNVD-202108-1241
	CNNVD-202108-1243
	CNNVD-202108-1259
HCC Embedded	CNNVD-202108-392
	CNNVD-202108-397
	CNNVD-202108-483
Horner Automation	CNNVD-202108-1246
	CNNVD-202108-1254
	CNNVD-202108-1262
Huawei	CNNVD-202108-114
	CNNVD-202108-116
	CNNVD-202108-118
	CNNVD-202108-321
Libssh组织	CNNVD-202108-2375
Linux基金会	CNNVD-202108-765
	CNNVD-202108-766
Microsoft	CNNVD-202108-834
	CNNVD-202108-875
Mozilla基金会	CNNVD-202108-712
	CNNVD-202108-713
	CNNVD-202108-714
	CNNVD-202108-715
	CNNVD-202108-716
	CNNVD-202108-718
	CNNVD-202108-719
	CNNVD-202108-720
	CNNVD-202108-721
	CNNVD-202108-723
	CNNVD-202108-727
	CNNVD-202108-734
	CNNVD-202108-895
	CNNVD-202108-898
	CNNVD-202108-899
	CNNVD-202108-906
	CNNVD-202108-908
Netgear	CNNVD-202108-959
	CNNVD-202108-1002
	CNNVD-202108-1009
	CNNVD-202108-1026
	CNNVD-202108-1036
Nvidia	CNNVD-202108-448
Pulse Secure	CNNVD-202108-457
Siemens	CNNVD-202108-941

	Totolink	CNNVD-202108-533	
	个人开发者	CNNVD-202108-1001	
		CNNVD-202108-1045	
		CNNVD-202108-1149	
		CNNVD-202108-1159	
		CNNVD-202108-1273	
		CNNVD-202108-1463	
		CNNVD-202108-1606	
		CNNVD-202108-1607	
		CNNVD-202108-1608	
		CNNVD-202108-1614	
		CNNVD-202108-1700	
		CNNVD-202108-1925	
		CNNVD-202108-1940	
		CNNVD-202108-1947	
		CNNVD-202108-2348	
访问控制错误	Cisco	CNNVD-202108-2355	ThroughTek Kalay Platform 访问控制错误漏洞（CNNVD-202108-1610）
		CNNVD-202108-2356	
	DELL	CNNVD-202108-1007	
	Hedgedoc团队	CNNVD-202108-2734	
	Intel	CNNVD-202108-1069	
	TYPO3	CNNVD-202108-978	
	ThroughTek	CNNVD-202108-1610	
	Tranquil	CNNVD-202108-1483	
	VMware	CNNVD-202108-2300	
	WordPress基金会	CNNVD-202108-778	
	个人开发者	CNNVD-202108-920	
		CNNVD-202108-1658	
资源管理错误	Apache基金会	CNNVD-202108-1621	Google Chrome 资源管理错误漏洞（CNNVD-202108-2810）
	FFmpeg	CNNVD-202108-1047	
	Fortinet	CNNVD-202108-344	
	Foxit	CNNVD-202108-1125	
	Google	CNNVD-202108-094	
		CNNVD-202108-1237	
		CNNVD-202108-1514	
		CNNVD-202108-2803	
		CNNVD-202108-2805	
		CNNVD-202108-2807	
		CNNVD-202108-2810	
	Huawei	CNNVD-202108-326	
		CNNVD-202108-979	
	Microsoft	CNNVD-202108-1510	
		CNNVD-202108-1512	
		CNNVD-202108-1513	
	Mozilla基金会	CNNVD-202108-739	
		CNNVD-202108-903	

	Qualcomm	CNNVD-202108-044	
	Siemens	CNNVD-202108-940	
		CNNVD-202108-957	
	个人开发者	CNNVD-202108-1099	
		CNNVD-202108-1594	
		CNNVD-202108-1695	
输入验证错误	Adobe	CNNVD-202108-1554	GitLab 输入验证错误漏洞 （CNNVD-202108-382）
		CNNVD-202108-1555	
	Cisco	CNNVD-202108-2303	
	GitLab	CNNVD-202108-382	
	Google	CNNVD-202108-1251	
		CNNVD-202108-1252	
	HCC Embedded	CNNVD-202108-387	
		CNNVD-202108-416	
		CNNVD-202108-499	
	Huawei	CNNVD-202108-101	
		CNNVD-202108-113	
		CNNVD-202108-125	
		CNNVD-202108-130	
		CNNVD-202108-320	
		CNNVD-202108-324	
	Intel	CNNVD-202108-1042	
		CNNVD-202108-1071	
	Linux基金会	CNNVD-202108-703	
	MB CONNECT LINE	CNNVD-202108-073	
	MONITORAPP	CNNVD-202108-1187	
	Microsoft	CNNVD-202108-847	
	Mozilla基金会	CNNVD-202108-913	
	Nagios	CNNVD-202108-1363	
	Nvidia	CNNVD-202108-445	
	OpenMage	CNNVD-202108-2637	
		CNNVD-202108-2638	
	Raonwiz	CNNVD-202108-510	
	Shopware	CNNVD-202108-1478	
	Sourceforge组织	CNNVD-202108-1944	
	个人开发者	CNNVD-202108-137	
		CNNVD-202108-371	
		CNNVD-202108-373	
		CNNVD-202108-531	
		CNNVD-202108-708	
		CNNVD-202108-918	
		CNNVD-202108-921	
		CNNVD-202108-923	
		CNNVD-202108-925	
		CNNVD-202108-931	
		CNNVD-202108-933	

		CNNVD-202108-936 CNNVD-202108-951 CNNVD-202108-972 CNNVD-202108-1028 CNNVD-202108-1429 CNNVD-202108-1431 CNNVD-202108-1438 CNNVD-202108-1444 CNNVD-202108-1452 CNNVD-202108-1455 CNNVD-202108-1458 CNNVD-202108-1461 CNNVD-202108-1479 CNNVD-202108-1493 CNNVD-202108-1517 CNNVD-202108-1518 CNNVD-202108-1519 CNNVD-202108-1520 CNNVD-202108-1521 CNNVD-202108-1522 CNNVD-202108-1523 CNNVD-202108-1524 CNNVD-202108-1525 CNNVD-202108-1526 CNNVD-202108-1527 CNNVD-202108-1528 CNNVD-202108-1529 CNNVD-202108-1530 CNNVD-202108-1531 CNNVD-202108-1532 CNNVD-202108-1533 CNNVD-202108-1534 CNNVD-202108-1611	

1. Fortinet FortiSandbox SQL 注入漏洞（CNNVD-202108-299）

Fortinet FortiSandbox 是美国飞塔（Fortinet）公司的一款 APT（高级持续性威胁）防护设备。该设备提供双重沙盒技术、动态威胁智能系统、实时控制面板和报告等功能。

Fortinet FortiSandbox 存在 SQL 注入漏洞，该漏洞源于产品未能过滤输入数据中的特殊字符。攻击者可通过该漏洞执行非法 SQL 语句。以下产品及版本受到影响： Fortinet FortiSandbox 3.1.0 至 3.1.4，

Fortinet FortiSandbox 3.2.0 至 3.2.1 版本。

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://www.fortiguard.com/psirt/FG-IR-20-171

2. Google TensorFlow 代码问题漏洞（CNNVD-202108-1260）

Google TensorFlow 是美国谷歌（Google）公司的一套用于机器学习的端到端开源平台。

TensorFlow 中存在代码问题漏洞，该漏洞源于产品从 YAML 格式反序列化到 Keras 模型时未对输入数据做有效验证，攻击者可通过该漏洞导致代码执行。以下产品及版本收到影响：TensorFlow 2.5.1、TensorFlow 2.4.3 和 TensorFlow 2.3.4。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://github.com/tensorflow/tensorflow/security/advisories/GHSA-r6jx-9g48-2r5r

3. 多款 Qualcomm 产品授权问题漏洞（CNNVD-202108-067）

Qualcomm 芯片是美国高通（Qualcomm）公司的芯片。一种将电路（主要包括半导体设备，也包括被动组件等）小型化的方式，并时常制造在半导体晶圆表面上。

Qualcomm Technologies 多款组件存在授权问题漏洞，该漏洞源于在四向握手期间对非 EAPOL/WAPI 纯文本帧的不当身份验证可能导致任意网络数据包注入。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=31fe5bb94f737ed98c41b5293d7e52485131ce32

4. Palo Alto Networks PAN-OS 操作系统命令注入漏洞（CNNVD-202108-1089）

Palo Alto Networks PAN-OS 是美国 Palo Alto Networks 公司的一

套为其防火墙设备开发的操作系统。

Palo Alto Networks PAN-OS web 存在操作系统命令注入漏洞，该漏洞源于 Palo Alto Networks PAN-OS web 界面上存在一个操作系统命令注入漏洞。攻击者可利用该漏洞执行任意的操作系统命令来提升权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://security.paloaltonetworks.com/CVE-2021-3050

5. F5 BIG-IP 缓冲区错误漏洞（CNNVD-202108-2295）

F5 BIG-IP 是美国 F5 公司的一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。

F5 BIG-IP 的 iRules 解析器存在缓冲区错误漏洞，攻击者可利用该漏洞触发拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://github.com/envoyproxy/envoy/security/advisories/GHSA-5vhv-gp9v-42qv

6. ThroughTek Kalay Platform 访问控制错误漏洞（CNNVD-202108-1610）

throughtek ThroughTek Kalay Platform 是中国物联智慧股份有限公司（throughtek）公司的一个应用软件。利用 P2P 技术启用 Kalay Cloud Platform 服务。

ThroughTek Kalay Platform 中存在访问控制错误漏洞，该漏洞源于产品网络允许通过 20 字节的 UUID 冒充 ThroughTek 设备。攻击者可通过该漏洞获得用户的访问凭据。以下产品及版本受到影响：ThroughTek Kalay P2P SDK 3.1.5 版本及之前版本。

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://www.throughtek.com

7. Google Chrome 资源管理错误漏洞（CNNVD-202108-2810）

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

Google Chrome 中存在资源管理错误漏洞，该漏洞源于产品的 Sign-In 未对内存资源进行检查。攻击者可通过该漏洞引用已经释放资源的地址。

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/2021/08/stable-channel-update-for-desktop_31.html

8. GitLab 输入验证错误漏洞（CNNVD-202108-382）

GitLab 是美国 GitLab 公司的一款使用 Ruby on Rails 开发的、自托管的、Git（版本控制系统）项目仓库应用程序。该程序可用于查阅项目的文件内容、提交历史、Bug 列表等。

GitLab 存在输入验证错误漏洞，该漏洞源于 OAuth 客户端 ID 处理不当，新订阅会在不正确的 OAuth 客户端应用程序上生成 OAuth 令牌。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://about.gitlab.com/releases/2021/08/03/security-release-gitlab-14-1-2-released/

二、漏洞平台推送情况

本月漏洞平台推送漏洞 24625 个。

表 7 2021 年 8 月漏洞平台推送情况

序号	漏洞平台	漏洞总量
1	漏洞盒子	4115
2	补天平台	20510
推送总计		24625

三、接报漏洞情况

本月接报漏洞 4040 个，其中信息技术产品漏洞（通用型漏洞）

479 个，网络信息系统漏洞（事件型漏洞）3561 个。

表 8 2021 年 8 月漏洞接报情况

序号	报送单位	漏洞总量
1	北京山石网科信息技术有限公司	1417
2	北京华云安信息技术有限公司	723
3	河南听潮盛世信息技术有限公司	334
4	杭州海康威视数字技术股份有限公司	244
5	北京安帝科技有限公司	134
6	杭州默安科技有限公司	128
7	北京天地和兴科技有限公司	112
8	北京数字观星科技有限公司	93
9	南京众智维信息科技有限公司	90
10	任子行网络技术股份有限公司	76
11	西安四叶草信息技术有限公司	46
12	太极计算机股份有限公司	40
13	远江盛邦（北京）网络安全科技股份有限公司	37
14	北京启明星辰信息安全技术有限公司	34
15	内蒙古中叶信息技术有限责任公司	32
16	山东新潮信息技术有限公司	31
17	亚信科技（成都）有限公司	30
18	山东云天安全技术有限公司	30
19	广东网安科技有限公司	22
20	星云博创科技有限公司	20
21	新华三技术有限公司	20
22	广州锦行网络科技有限公司	20
23	中兴通讯股份有限公司	20
24	华为技术有限公司	19
25	广州竞远安全技术股份有限公司	18
26	浙江宇视科技有限公司	18
27	安徽长泰信息安全服务有限公司	17
28	浙江大华技术股份有限公司	16
29	北京云测信息技术有限公司	15
30	北京天融信网络安全技术有限公司	14
31	杭州迪普科技股份有限公司	14
32	清华大学网络科学与网络空间研究院	13
33	北京众安天下科技有限公司	13
34	福建经联网络技术有限公司	11
35	长春嘉诚信息技术股份有限公司	10
36	个人	10
37	天津市兴先道科技有限公司	10

38	西安交大捷普网络科技有限公司	10
39	安全能力生态聚合(北京)运营科技有限公司	8
40	恒安嘉新（北京）科技股份公司	7
41	海南神州希望网络有限公司	7
42	广州易东信息安全技术有限公司	7
43	中国电信集团系统集成有限责任公司	7
44	上海安识网络科技有限公司	6
45	腾讯科技（北京）有限公司	6
46	网神信息技术（北京）股份有限公司	6
47	杰润鸿远（北京）科技有限公司	5
48	安徽华云网安信息技术有限公司	5
49	中电长城网际系统应用有限公司	5
50	北京优炫软件股份有限公司	4
51	北京安天网络安全技术有限公司	4
52	北京机沃科技有限公司	3
53	上海斗象信息科技有限公司	2
54	阿里巴巴（中国）网络技术有限公司	2
55	厦门服云信息科技有限公司	2
56	浙江国利网安科技有限公司	2
57	杭州美创科技有限公司	2
58	北京智游网安科技有限公司	1
59	杭州安恒信息技术股份有限公司	1
60	北京京东尚科信息技术有限公司	1
61	广州大学	1
62	中通服咨询设计研究院有限公司	1
63	内蒙古思沃科技有限公司	1
64	南京赛宁信息技术有限公司	1
65	北京安信天行科技有限公司	1
66	年华数据科技（成都）有限公司	1
报送总计		4040

四、重大漏洞预警

4.1 微软多个安全漏洞的预警

近日，微软官方发布了多个安全漏洞的公告，包括Microsoft Windows TCP/IP component 缓冲区错误漏洞（CNNVD-202108-856、CVE-2021-26424 ）、Microsoft Windows 代码注入漏洞

（CNNVD-202108-863、CVE-2021-26432）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据，提升权限等。微软多个产品和系统受漏洞影响。目前，微软官方已经发布漏洞修复补丁，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

2021 年 8 月 11 日，微软发布了 2021 年 8 月份安全更新，共 44 个漏洞的补丁程序，CNNVD对这些漏洞进行了收录。本次更新主要涵盖了Windows操作系统、Microsoft Graphics Component、Remote Desktop Client、Windows NTLM、Windows TCP/IP、Windows Update Assistant等。CNNVD对其危害等级进行了评价，其中超危漏洞 2 个、高危漏洞有 26 个，中危漏洞 16 个。微软多个产品和系统版本受漏洞影响，具体影响范围可访问 https://portal.msrc.microsoft.com/zh-cn/security-guidance 查询。

. 漏洞详情

此次更新共包括 44 个漏洞的补丁程序，其中超危漏洞 2 个、高危漏洞有 26 个，中危漏洞 16 个。

序号	漏洞名称	CNNVD 编号	CVE 编号	危害等级	官方链接
1	Microsoft Windows TCP/IP component 缓冲区错误漏洞	CNNVD-202108-856	CVE-2021-26424	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26424

2	Microsoft Windows 代码注入漏洞	CNNVD-202108-863	CVE-2021-26432	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26432
3	Microsoft Windows Update Assistant 缓冲区错误漏洞	CNNVD-202108-834	CVE-2021-36948	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36948
4	Microsoft Windows Print Spooler Components 代码注入漏洞	CNNVD-202108-835	CVE-2021-36947	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36947
5	Microsoft Windows 安全漏洞	CNNVD-202108-836	CVE-2021-36942	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942
6	Microsoft Windows Print Spooler Components 代码注入漏洞	CNNVD-202108-837	CVE-2021-36936	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36936
7	Microsoft Windows Codecs 代码注入漏洞	CNNVD-202108-838	CVE-2021-36937	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36937
8	Microsoft Windows 信息泄露漏洞	CNNVD-202108-840	CVE-2021-36933	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36933
9	Microsoft Windows Media Foundation 权限许可和访问控制问题漏洞	CNNVD-202108-841	CVE-2021-36927	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36927
10	Microsoft Windows Bluetooth Service 权限许可和访问控制问题漏洞	CNNVD-202108-842	CVE-2021-34537	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34537
11	Microsoft Windows 信息泄露漏洞	CNNVD-202108-843	CVE-2021-36932	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36932

12	Microsoft Dynamics 代码注入漏洞	CNNVD-202108-844	CVE-2021-34524	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34524
13	Microsoft Windows 信息泄露漏洞	CNNVD-202108-845	CVE-2021-36926	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36926
14	Microsoft Windows Storage Spaces Controller 权限许可和访问控制问题漏洞	CNNVD-202108-850	CVE-2021-34536	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34536
15	Microsoft Remote Desktop Protocol Client 代码注入漏洞	CNNVD-202108-851	CVE-2021-34535	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34535
16	Microsoft Windows Print Spooler Components 权限许可和访问控制问题漏洞	CNNVD-202108-853	CVE-2021-34483	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34483
17	Microsoft Graphics Components 代码注入漏洞	CNNVD-202108-854	CVE-2021-34530	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34530
18	Microsoft Windows 产品权限许可和访问控制问题漏洞	CNNVD-202108-855	CVE-2021-34484	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34484
19	Microsoft Graphics Components 代码注入漏洞	CNNVD-202108-857	CVE-2021-34533	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34533
20	Microsoft Office 代码注入漏洞	CNNVD-202108-859	CVE-2021-34478	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34478
21	Microsoft Windows Event Tracing 权限许可和访问控制问题漏洞	CNNVD-202108-864	CVE-2021-34487	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34487

22	Microsoft Windows Update Assistant 权限许可和访问控制问题漏洞	CNNVD-202108-866	CVE-2021-26431	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26431
23	Microsoft Office 和 Microsoft SharePoint 安全漏洞	CNNVD-202108-868	CVE-2021-36940	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36940
24	Microsoft Office 代码注入漏洞	CNNVD-202108-870	CVE-2021-36941	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36941
25	Microsoft Azure Sphere 权限许可和访问控制问题漏洞	CNNVD-202108-871	CVE-2021-26429	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26429
26	Microsoft Windows 权限许可和访问控制问题漏洞	CNNVD-202108-873	CVE-2021-26426	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26426
27	Microsoft Windows Event Tracing 权限许可和访问控制问题漏洞	CNNVD-202108-874	CVE-2021-26425	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26425
28	Microsoft Azure 和 Microsoft Azure Active Directory Connect 授权问题漏洞	CNNVD-202108-877	CVE-2021-36949	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36949
29	Microsoft Windows Cryptographic Services 信息泄露漏洞	CNNVD-202108-839	CVE-2021-36938	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36938
30	Microsoft Dynamics 跨站脚本漏洞	CNNVD-202108-846	CVE-2021-36950	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36950
31	Microsoft .NET Core 和 Microsoft Visual	CNNVD-202108-847	CVE-2021-26423	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26423

	Studio 输入验证错误漏洞				
32	Microsoft .NET Core 和 Microsoft Visual Studio 信息泄露漏洞	CNNVD-202108-848	CVE-2021-34485	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34485
33	Microsoft .NET Core 和 Microsoft Visual Studio 信息泄露漏洞	CNNVD-202108-849	CVE-2021-34532	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34532
34	Microsoft Windows Update Assistant 权限许可和访问控制问题漏洞	CNNVD-202108-852	CVE-2021-36945	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36945
35	Microsoft Azure 权限许可和访问控制问题漏洞	CNNVD-202108-858	CVE-2021-36943	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36943
36	Microsoft Windows MSHTML Platform 代码注入漏洞	CNNVD-202108-860	CVE-2021-34534	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34534
37	Microsoft Azure 权限许可和访问控制问题漏洞	CNNVD-202108-861	CVE-2021-33762	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-33762
38	Microsoft Windows 信息泄露漏洞	CNNVD-202108-862	CVE-2021-26433	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26433
39	Microsoft Windows Defender 权限许可和访问控制问题漏洞	CNNVD-202108-865	CVE-2021-34471	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34471
40	Microsoft Windows Event Tracing 权限许	CNNVD-202108-867	CVE-2021-34486	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34486

	可和访问控制问题漏洞				
41	Microsoft Azure Sphere 输入验证错误漏洞	CNNVD-202108-869	CVE-2021-26428	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26428
42	Microsoft Azure Sphere 输入验证错误漏洞	CNNVD-202108-872	CVE-2021-26430	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26430
43	多款 Microsoft 产品缓冲区错误漏洞	CNNVD-202108-875	CVE-2021-34480	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34480
44	Microsoft Dynamics 跨站脚本漏洞	CNNVD-202108-876	CVE-2021-36946	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36946

. 修复建议

目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认漏洞影响，尽快采取修补措施。微软官方补丁下载地址：

https://msrc.microsoft.com/update-guide/en-us

4.2 SonicWall SRA/SMA SQL 注入漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于SonicWall Analytics 配置错误漏洞（CNNVD-202108-938、CVE-2021-20032）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远程执行恶意代码，并最终控制目标设备。SonicWall Analytics 2.5.2518 及其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 Analytics是美国SonicWall公司的一款适用于网络的高性能管理和报告引擎。该漏洞是由于Java 调试线协议 (JDWP) 接口安全配置错误导致，攻击者可利用该漏洞可在未授权的情况下，构造恶意数据远程执行恶意代码，最终控制目标设备。

. 危害影响

成功利用漏洞的攻击者可以在未授权的情况下远程执行恶意代码，并最终控制目标设备。SonicWall Analytics 2.5.2518 及其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://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0018