北京师范大学网络信息安全通告

2021 年 2 月报告

北京师范大学信息网络中心

2021 年 3 月

信息安全漏洞周报

（2021 年 2月　　第 1 周）

CNNVD　　2020 年 2 月 7 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2021 年 2 月 1 日至 2021 年 2 月 7 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 474 个，与上周（326 个）相比增加了 45.40%。

接报漏洞情况

本周 CNNVD 接报漏洞 2227 个，其中信息技术产品漏洞（通用型漏洞）99 个，网络信息系统漏洞（事件型漏洞）2128 个。

重大漏洞预警

Sonicwall SMA100 SQL 注入漏洞（CNNVD-202102-394）：成功利用漏洞的攻击者可以在未授权的情况下远程控制目标设备。Sonic SMA 10.2.0.5 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。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞 474 个，漏洞新增数量有所上升。从厂商分布来看苹果公司新增漏洞最多，有 64 个；从漏洞类型来看，访问控制错误类的安全漏洞占比最大，达到 8.23%。新增漏洞中，超危漏洞 54 个，高危漏洞 158 个，中危漏洞 254 个，低危漏洞 8 个。相应修复率分别为 72.22%、94.94%、94.88%和 100.00%。根据补丁信息统计，合计 438 个漏洞已有修复补丁发布，整体修复率为 92.41%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 474 与上周（326 个）相比增多了 45.40%。

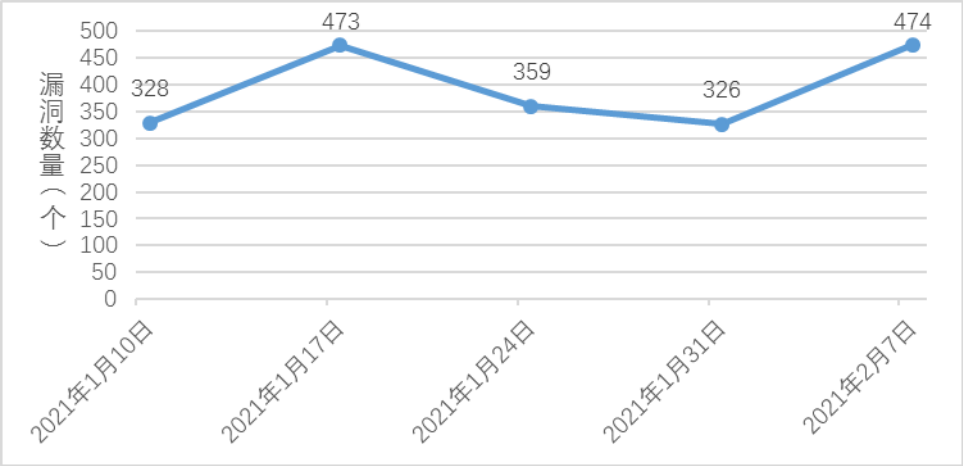

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，苹果公司新增漏洞最多，有 64 个。各厂商漏洞数量分布如表 1 所示。

表 1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量（个）	所占比例
1	苹果	64	13.50%
2	思科	56	11.81%
3	谷歌	50	10.55%
4	Qualcomm	29	6.12%
5	JetBrains	26	5.49%

本周国内厂商漏洞 24 个，华为公司漏洞数量最多，有 15 个。国内厂商漏洞整体修复率为 75.00%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看，访问控制错误类的安全漏洞占比最大，达到 8.23%。漏洞类型统计如表 2 所示。

表 2 漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	访问控制错误	39	8.23%
2	缓冲区错误	36	7.59%
3	信息泄露	29	6.12%
4	资源管理错误	29	6.12%
5	输入验证错误	26	5.49%
6	跨站脚本	23	4.85%
7	代码问题	17	3.59%
8	授权问题	17	3.59%
9	SQL 注入	13	2.74%
10	命令注入	10	2.11%
11	路径遍历	7	1.48%
12	跨站请求伪造	6	1.27%
13	操作系统命令注入	5	1.05%
14	注入	5	1.05%
15	加密问题	3	0.63%
16	权限许可和访问控制问题	2	0.42%
17	信任管理问题	2	0.42%
18	数据伪造问题	2	0.42%
19	数字错误	2	0.42%
20	代码注入	1	0.21%
21	安全特征问题	1	0.21%

22	其他	198	41.77%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 54 个，高危漏洞 158 个，中危漏洞 254 个，低危漏洞 8 个。相应修复率分别为 72.22%、94.94%、94.88%和 100.00%。根据补丁信息统计，合计 438 个漏洞已有修复补丁发布，整体修复率为 92.41%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	54	39	72.22%
2	高危	158	150	94.94%
3	中危	254	241	94.88%
4	低危	8	8	100.00%
合计		474	438	92.41%

（四） 本周重要漏洞实例

本期重要漏洞实例如表 4 所示。

表 4 本期重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	SQL 注入	CNNVD-202102-394	Sonicwall	Sonicwall SMA100 SQL 注入漏洞	是	超危
2	其他	CNNVD-202102-065	苹果	Apple Safari WebKit 安全漏洞	是	高危
3	其他	CNNVD-202102-271	谷歌	Google Chrome 安全漏洞	是	高危

1. Sonicwall SMA100 SQL 注入漏洞（CNNVD-202102-394）

Sonicwall SMA100 是美国 Sonicwall 公司的一款安全访问网关设备。

SonicWall SSLVPN SMA100 product 存在 SQL 注入漏洞，该漏洞允许远程未经身份验证的攻击者执行 SQL 查询访问用户名密码和其他会话相关信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001

2. Apple Safari WebKit 安全漏洞（CNNVD-202102-065）

Apple Safari 是美国苹果（Apple）公司的一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。

Safari 14.0.3 WebKit 存在安全漏洞，该漏洞源于恶意制作的 web 内容可能导致任意代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.apple.com/en-us/HT212146

3. Google Chrome 安全漏洞（CNNVD-202102-271）

Google Chromium 是美国谷歌（Google）的一款开源的 Web 浏览器。

Google Chromium 存在安全漏洞，该漏洞源于“扩展”中的堆缓冲区溢出。以下产品和版本受到影响：Microsoft Edge (Chromium-based)。

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/2021/02/stable-channel-update-for-desktop.html

二、接报漏洞情况

本周 CNNVD 接报漏洞 2227 个，其中信息技术产品漏洞（通用型漏洞）99 个，网络信息系统漏洞（事件型漏洞）2128 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	上海斗像信息科技有限公司	1327
2	网神信息技术（北京）股份有限公司	685
3	北京天地和兴科技有限公司	49
4	北京启明星辰信息安全技术有限公司	30
5	北京数字观星科技有限公司	21
6	山东华鲁科技发展股份有限公司	15
7	任子行信息技术有限公司	13
8	南京众智维信息科技有限公司	10
9	北京天融信网络安全技术有限公司	8
10	北京梆梆安全科技有限公司	8
11	山东云天安全技术有限公司	8
12	绿盟科技集团股份有限公司安全研究部	7
13	北京圣博润高新技术股份有限公司	6
14	广州竞远安全技术股份有限公司	6
15	北京机沃科技有限公司	4
16	深信服科技股份有限公司	4
17	个人	3
18	中兴通讯	3
19	北京威努特技术有限公司	3

20	博智安全科技股份有限公司	3
21	恒安嘉新（北京）科技股份公司	3
22	浪潮电子信息产业股份有限公司	3
23	深圳市魔方安全科技有限公司	2
24	北京惠而特科技有限公司	1
25	北京时代新威信息技术有限公司	1
26	北京智游网安科技有限公司	1
27	华为未然实验室	1
28	北京山石网科信息技术有限公司	1
29	海南神州希望网络有限公司	1
报送总计		2227

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 102 份。

序号	报送单位	预警总量
1	深信服科技股份有限公司	22
2	杭州迪普科技股份有限公司	13
3	北京启明星辰信息安全技术有限公司	10
4	北京华云安信息技术有限公司	7
5	北京华顺信安科技有限公司	6
6	网神信息技术（北京）股份有限公司	5
7	北京知道创宇信息技术股份有限公司	5
8	北京山石网科信息技术有限公司	5
9	北京奇虎科技有限公司	5

10	博智安全科技股份有限公司	4
11	浪潮电子信息产业股份有限公司	3
12	任子行网络技术股份有限公司	3
13	新华三技术有限公司	3
14	内蒙古洞明科技有限公司	2
15	北京天融信网络安全技术有限公司	2
16	北京中测安华科技有限公司	2
17	杭州安恒信息技术股份有限公司	2
18	北京安天网络安全技术有限公司	1
19	内蒙古奥创科技有限公司	1
20	远江盛邦(北京)网络安全科技股份有限公司	1
报送总计		102

四、重大漏洞预警

Sonicwall SMA100 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 SMA100 SQL 注入漏洞（CNNVD-202102-394、CVE-2021-20016）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控制目标设备。Sonic SMA 10.2.0.5 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 SMA100 是美国 Sonicwall 公司的一款安全访问网关设备。SonicWall SSLVPN SMA100 product 存在 SQL 注入漏洞，该漏洞允许远程未经身份验证的攻击者执行 SQL 查询访问用户名密码和其他会话相关信息，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远程控制目标设备。Sonic SMA 10.2.0.5 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-2021-0001

信息安全漏洞周报

（2021 年 2 月　　第 2 周）

CNNVD　　2020 年 2 月 14 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2021 年 2 月 8 日至 2021 年 2 月 14 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 553 个，与上周（474 个）相比增加了 16.67%。

接报漏洞情况

本周 CNNVD 接报漏洞 1376 个，其中信息技术产品漏洞（通用型漏洞）28 个，网络信息系统漏洞（事件型漏洞）1348 个。

重大漏洞预警

微软多个安全漏洞：包括 Windows TCP/IP 安全漏洞（CNNVD-202102-719、CVE-2021-24094）、Microsoft Excel 安全漏洞（CNNVD-202102-693、CVE-2021-24069）等。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。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞 553 个，漏洞新增数量有所上升。从厂商分布来看 Intel 公司新增漏洞最多，有 58 个；从漏洞类型来看，缓冲区错误类的安全漏洞占比最大，达到 15.91%。新增漏洞中，超危漏洞 92 个，高危漏洞 251 个，中危漏洞 179 个，低危漏洞 31 个。相应修复率分别为 90.22%、95.22%、88.27%和 96.77%。根据补丁信息统计，合计 510 个漏洞已有修复补丁发布，整体修复率为 92.22%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 553 与上周（474 个）相比增多了 16.67%。

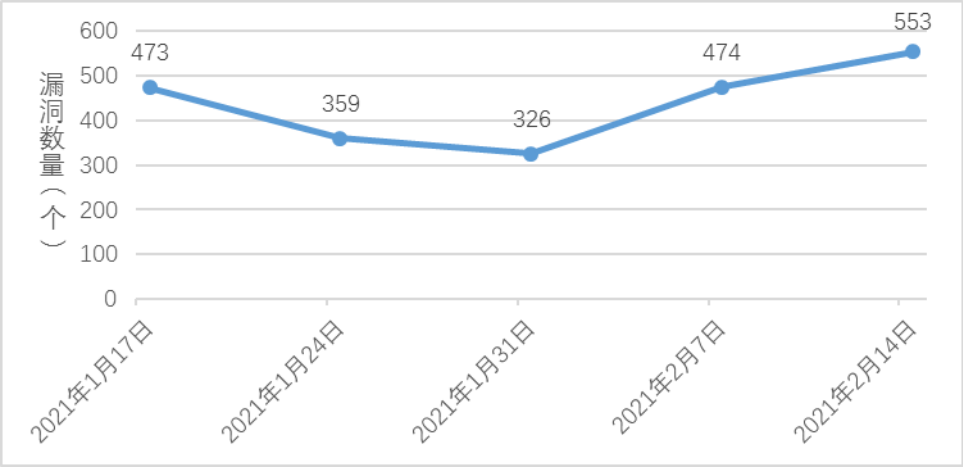

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Intel 公司新增漏洞最多，有 58 个。各厂商漏洞数量分布如表 1 所示。

表 1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量（个）	所占比例
1	Intel	58	10.49%
2	微软	57	10.31%
3	Adobe	46	8.32%
4	福昕	23	4.16%
5	IBM	22	3.98%

本周国内厂商漏洞 36 个，福昕公司漏洞数量最多，有 23 个。国内厂商漏洞整体修复率为 94.44%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看，缓冲区错误类的安全漏洞占比最大，达到 15.91%。漏洞类型统计如表 2 所示。

表 2 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	88	15.91%
2	跨站脚本	35	6.33%
3	信任管理问题	32	5.79%
4	代码问题	30	5.42%
5	输入验证错误	29	5.24%
6	信息泄露	28	5.06%
7	资源管理错误	28	5.06%
8	访问控制错误	23	4.16%
9	授权问题	17	3.07%
10	权限许可和访问控制问题	14	2.53%
11	路径遍历	12	2.17%
12	SQL 注入	11	1.99%
13	安全特征问题	11	1.99%
14	命令注入	8	1.45%
15	注入	8	1.45%
16	跨站请求伪造	7	1.27%

17	操作系统命令注入	6	1.08%
18	代码注入	6	1.08%
19	加密问题	5	0.90%
20	默认配置问题	5	0.90%
21	日志信息泄露	3	0.54%
22	数据伪造问题	2	0.36%
23	处理逻辑错误	2	0.36%
24	数字错误	1	0.18%
25	环境问题	1	0.18%
26	参数注入	1	0.18%
27	其他	137	24.77%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 92 个，高危漏洞 251 个，中危漏洞 179 个，低危漏洞 31 个。相应修复率分别为 90.22%、95.22%、88.27%和 96.77%。根据补丁信息统计，合计 510 个漏洞已有修复补丁发布，整体修复率为 92.22%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	92	83	90.22%
2	高危	251	239	95.22%
3	中危	179	158	88.27%
4	低危	31	30	96.77%
合计		553	510	92.22%

（四） 本周重要漏洞实例

本期重要漏洞实例如表 4 所示。

表 4 本期重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	其他	CNNVD-202102-700	微软	Microsoft Windows TCP/IP 安全漏洞	是	超危
2	其他	CNNVD-202102-650	Linux 基金会	Linux kernel 安全漏洞	是	高危

3	访问控制错误	CNNVD-202102-757	Adobe	Acrobat Reader DC 访问控制错误漏洞	是	高危

1. Microsoft Windows TCP/IP 安全漏洞（CNNVD-202102-700）

Microsoft Windows TCP/IP component 是美国微软（Microsoft）公司的一个为 Windows 提供 TCP/IP 配置功能的组件。

Microsoft Windows TCP/IP 中存在安全漏洞。以下产品和版本受到影响：Windows 10 Version 1803 for 32-bit Systems,Windows 10 Version 1803 for x64-based Systems,Windows 10 Version 1803 for ARM64-based Systems,Windows 10 Version 1809 for 32-bit Systems,Windows 10 Version 1809 for x64-based Systems,Windows 10 Version 1809 for ARM64-based Systems,Windows Server 2019,Windows Server 2019 (Server Core installation),Windows 10 for 32-bit Systems,Windows 10 for x64-based Systems,Windows 10 Version 1607 for 32-bit Systems,Windows 10 Version 1607 for x64-based Systems,Windows Server 2016,Windows Server 2016 (Server Core installation),Windows 7 for 32-bit Systems Service Pack 1,Windows 7 for x64-based Systems Service Pack 1,Windows 8.1 for 32-bit systems,Windows 8.1 for x64-based systems,Windows RT 8.1,Windows Server 2008 for 32-bit Systems Service Pack 2,Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation),Windows Server 2008 for

x64-based Systems Service Pack 2,Windows Server 2008 for x64-based Systems Service Pack 2 (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 (Server Core installation),Windows Server 2012,Windows Server 2012 (Server Core installation),Windows Server 2012 R2,Windows Server 2012 R2 (Server Core installation),Windows 10 Version 1909 for 32-bit Systems,Windows 10 Version 1909 for x64-based Systems,Windows 10 Version 1909 for ARM64-based Systems,Windows Server, version 1909 (Server Core installation),Windows 10 Version 2004 for 32-bit Systems,Windows 10 Version 2004 for ARM64-based Systems,Windows 10 Version 2004 for x64-based Systems,Windows Server, version 2004 (Server Core installation),Windows 10 Version 20H2 for x64-based Systems,Windows 10 Version 20H2 for 32-bit Systems,Windows 10 Version 20H2 for ARM64-based Systems,Windows Server, version 20H2 (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://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24074

2. Linux kernel 安全漏洞（CNNVD-202102-650）

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。

Linux Kernel 中存在安全漏洞，该漏洞源于 io_grab_files()强制使用释放的内存区域，从而触发拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://access.redhat.com/security/cve/cve-2021-20226

3. Acrobat Reader DC 访问控制错误漏洞（CNNVD-202102-757）

Adobe Acrobat Reader 是美国奥多比（Adobe）公司的一款 PDF 查看器。该软件用于打印，签名和注释 PDF。

Acrobat Reader DC 中存在访问控制错误漏洞，该漏洞源于网络系统或产品未正确限制来自未授权角色的资源访问。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://helpx.adobe.com/security/products/acrobat/apsb21-09.html

二、接报漏洞情况

本周 CNNVD 接报漏洞 1376 个，其中信息技术产品漏洞（通用型漏洞）28 个，网络信息系统漏洞（事件型漏洞）1348 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	上海斗像信息科技有限公司	759
2	网神信息技术（北京）股份有限公司	422
3	山东华鲁科技发展股份有限公司	45
4	北京数字观星科技有限公司	41

5	广州锦行网络科技有限公司	39
6	北京天地和兴科技有限公司	35
7	远江盛邦（北京）网络安全科技股份有限公司	10
8	北京云测信息技术有限公司	9
9	北京圣博润高新技术股份有限公司	6
10	广州竞远安全技术股份有限公司	3
11	个人	2
12	恒安嘉新（北京）科技股份公司	2
13	北京天融信网络安全技术有限公司	1
14	华为技术有限公司未然实验室	1
报送总计		1376

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 41 份。

序号	报送单位	预警总量
1	杭州迪普科技股份有限公司	21
2	深信服科技股份有限公司	5
3	北京奇虎科技有限公司	3
4	网神信息技术（北京）股份有限公司	2
5	远江盛邦(北京)网络安全科技股份有限公司	2
6	北京山石网科信息技术有限公司	2
7	北京安天网络安全技术有限公司	2
8	北京启明星辰信息安全技术有限公司	1
9	北京天融信网络安全技术有限公司	1

10	北京知道创宇信息技术股份有限公司	1
11	杭州安恒信息技术股份有限公司	1
报送总计		41

四、重大漏洞预警

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 Windows TCP/IP 安全漏洞（CNNVD-202102-719、CVE-2021-24094）、Microsoft Excel 安全漏洞（CNNVD-202102-693、CVE-2021-24069）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 2 月 10 日，微软发布了 2021 年 2 月份安全更新，共 56 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、Edge 浏览器、Office 办公套件、Skype、反病毒引擎、.NET 等多个 Windows 平台下应用软件和组件。CNNVD 对其危害等级进行了评价，其中包括 7 个超危漏洞，35 个高危漏洞。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 56 个漏洞的补丁程序，其中 7 个超危漏洞，35 个高危漏洞。

序号	cnnvd 漏洞名称	cnnvd 编号	危害等级	中文链接
1	Microsoft Windows TCP/IP 安全漏洞	CNNVD-202102-719	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24094
2	多款 Microsoft Windows 产品安全漏洞	CNNVD-202102-712	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24091
3	Microsoft Windows 本地后台处理程序安全漏洞	CNNVD-202102-710	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24088
4	Microsoft Windows DNS 服务器安全漏洞	CNNVD-202102-707	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24078
5	Microsoft Windows 传真服务安全漏洞	CNNVD-202102-702	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24077

6	Microsoft Windows TCP/IP 远程执行代码漏洞	CNNVD-202102-700	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24074
7	Microsoft Graphics Components 安全漏洞	CNNVD-202102-687	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24093
8	Microsoft .NET Framework 安全漏洞	CNNVD-202102-721	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24111
9	Microsoft 程序包管理器服务安全漏洞	CNNVD-202102-716	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24105
10	Microsoft Windows 事件跟踪服务安全特征问题漏洞	CNNVD-202102-715	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24103
11	多款 Microsoft 产品安全特征问题漏洞	CNNVD-202102-714	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24102
12	Microsoft Defender 安全特征问题漏洞	CNNVD-202102-713	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24092
13	Microsoft Windows TCP/IP 安全漏洞	CNNVD-202102-711	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24086

14	Microsoft Windows Mobile Device Management 信息泄露漏洞	CNNVD-202102-709	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24084
15	多款 Microsoft 产品安全漏洞	CNNVD-202102-708	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24083
16	Microsoft Windows Codecs 库 安全漏洞	CNNVD-202102-706	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24081
17	Microsoft Windows 备份引擎信息泄露漏洞	CNNVD-202102-703	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24079
18	Microsoft Skype 和 Microsoft Lync Server 安全漏洞	CNNVD-202102-698	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24073
19	Microsoft SharePoint 安全漏洞	CNNVD-202102-697	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24072
20	Microsoft SharePoint 安全漏洞	CNNVD-202102-696	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24071
21	Microsoft Excel 安全漏洞	CNNVD-202102-695	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24070

22	Microsoft Windows Installer 安全特征问题漏洞	CNNVD-202102-694	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1727
23	Microsoft Excel 安全漏洞	CNNVD-202102-693	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24069
24	Microsoft Excel 安全漏洞	CNNVD-202102-692	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24068
25	Microsoft SharePoint 安全漏洞	CNNVD-202102-691	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24066
26	Microsoft Excel 安全漏洞	CNNVD-202102-690	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24067
27	Microsoft Exchange Server 安全漏洞	CNNVD-202102-689	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1730
28	Microsoft SharePoint 安全漏洞	CNNVD-202102-686	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1726
29	Microsoft Visual Studio Code npm-script 插件安全漏洞	CNNVD-202102-684	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26700

30	Microsoft .NET Core 安全漏洞	CNNVD-202102-685	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26701
31	Microsoft .NET Core 安全漏洞	CNNVD-202102-681	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24112
32	Microsoft Windows 安全漏洞	CNNVD-202102-680	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24096
33	Microsoft Azure IoT CLI 授权问题漏洞	CNNVD-202102-679	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24087
34	Microsoft Windows PKU2U 安全特征问题漏洞	CNNVD-202102-675	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-25195
35	Microsoft Windows 传真服务安全漏洞	CNNVD-202102-676	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1722
36	Microsoft Win32k 安全特征问题漏洞	CNNVD-202102-677	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1698
37	Microsoft Windows 信息泄露漏洞	CNNVD-202102-672	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1734

38	Microsoft Sysinternals PsExec 安全特征问题漏洞	CNNVD-202102-673	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1733
39	Microsoft Windows Win32k 安全特征问题漏洞	CNNVD-202102-670	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1732
40	Microsoft PFX 安全特征问题漏洞	CNNVD-202102-674	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1731
41	Microsoft System Center Operations Manager 安全特征问题漏洞	CNNVD-202102-671	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1728
42	Microsoft Visual Studio 和 Visual Studio Code 安全漏洞	CNNVD-202102-668	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1639
43	Microsoft Azure Kubernetes Service 安全特征问题漏洞	CNNVD-202102-722	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24109
44	Microsoft Directx 信息泄露漏洞	CNNVD-202102-718	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24106
45	Microsoft Lync Server 安全漏洞	CNNVD-202102-720	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24099

46	Microsoft Windows 控制台驱动程序安全漏洞	CNNVD-202102-717	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24098
47	Microsoft PowerShell Utility 模块安全特征问题漏洞	CNNVD-202102-705	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24082
48	多款 Microsoft 产品安全漏洞	CNNVD-202102-704	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24080
49	Microsoft Windows 网络文件系统安全漏洞	CNNVD-202102-701	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24075
50	Microsoft Windows VMSwitch 信息泄露漏洞	CNNVD-202102-699	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24076
51	Microsoft Teams iOS 安全漏洞	CNNVD-202102-688	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24114
52	Microsoft Edge 信息泄露漏洞	CNNVD-202102-683	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24100
53	Microsoft Dynamics 365 信息泄露漏洞	CNNVD-202102-682	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24101

54	Microsoft Exchange Server 安全漏洞	CNNVD-202102-678	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24085
55	Microsoft Dynamics 跨站脚本漏洞	CNNVD-202102-669	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1724
56	Microsoft .NET Core 和 Microsoft Visual Studio 安全漏洞	CNNVD-202102-667	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1721

.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

信息安全漏洞周报

（2021 年 2月　　第 3 周）

CNNVD　　2020 年 2 月 21 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2021 年 2 月 15 日至 2021 年 2 月 21 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 255 个，与上周（553 个）相比减少了 53.89%。

接报漏洞情况

本周 CNNVD 接报漏洞 1493 个，其中信息技术产品漏洞（通用型漏洞）13 个，网络信息系统漏洞（事件型漏洞）1480 个。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞 255 个，漏洞新增数量有所下降。从厂商分布来看谷歌公司新增漏洞最多，有 9 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 9.02%。新增漏洞中，超危漏洞 20 个，高危漏洞 99 个，中危漏洞 127 个，低危漏洞 9 个。相应修复率分别为 80.00%、82.83%、70.87%和 100.00%。根据补丁信息统计，合计 197 个漏洞已有修复补丁发布，整体修复率为 77.25%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 255 与上周（553 个）相比减少了 53.89%。

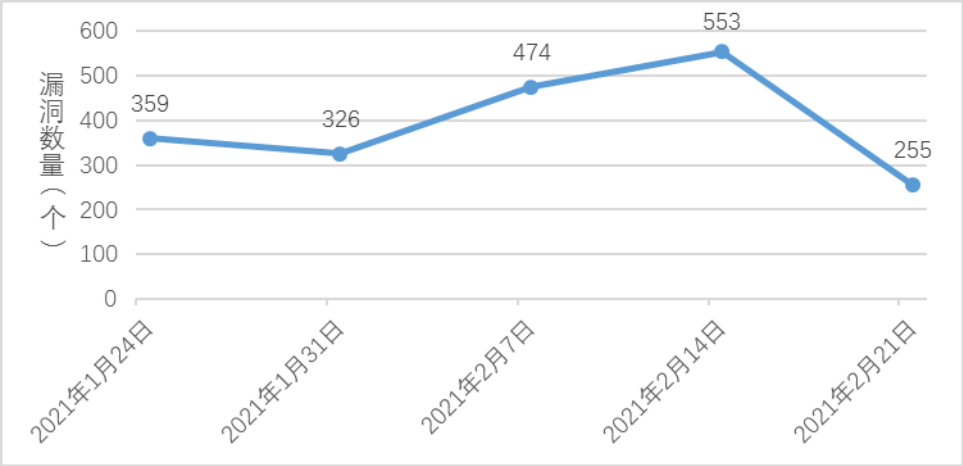

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，谷歌公司新增漏洞最多，有 9 个。各厂商漏洞数量分布如表 1 所示。

表 1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量（个）	所占比例
1	谷歌	9	3.53%
2	IBM	6	2.35%
3	Red Hat	6	2.35%
4	Linux 基金会	6	2.35%
5	西科姆	6	2.35%

本周国内厂商漏洞 16 个，研华公司漏洞数量最多，有 6 个。国内厂商漏洞整体修复率为 87.50%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 9.02%。漏洞类型统计如表 2 所示。

表 2 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	23	9.02%
2	SQL 注入	18	7.06%
3	缓冲区错误	14	5.49%
4	信息泄露	12	4.71%
5	权限许可和访问控制问题	11	4.31%
6	路径遍历	11	4.31%
7	输入验证错误	9	3.53%
8	访问控制错误	7	2.75%
9	命令注入	7	2.75%
10	操作系统命令注入	7	2.75%
11	代码问题	6	2.35%
12	资源管理错误	6	2.35%
13	跨站请求伪造	6	2.35%
14	注入	5	1.96%
15	授权问题	3	1.18%
16	信任管理问题	1	0.39%
17	代码注入	1	0.39%
18	加密问题	1	0.39%
19	数据伪造问题	1	0.39%
20	其他	105	41.18%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 20 个，高危漏洞 99 个，中危漏洞 127 个，低危漏洞 9 个。相应修复率分别为 80.00%、82.83%、70.87%和 100.00%。根据补丁信息统计，合计 197 个漏洞已有修复补丁发布，整体修复率为 77.25%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	20	16	80.00%
2	高危	99	82	82.83%
3	中危	127	90	70.87%
4	低危	9	9	100.00%
合计		255	197	77.25%

（四） 本周重要漏洞实例

本期重要漏洞实例如表 4 所示。

表 4 本期重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	操作系统命令注入	CNNVD-202102-1249	Accellion	Accellion FTA 操作系统命令注入漏洞	是	超危
2	操作系统命令注入	CNNVD-202102-1136	Nagios	Nagios XI 操作系统命令注入漏洞	是	高危
3	数据伪造问题	CNNVD-202102-1301	思科	思科 Cisco AnyConnect Secure Mobility Client 数据伪造问题漏洞	是	高危

1. Accellion FTA 操作系统命令注入漏洞（CNNVD-202102-1249）

Accellion FTA 是美国 Accellion 公司的一个企业内容防火墙。提供了一个防止来自第三方网络风险的数据泄露和违规行为。

Accellion FTA 中存在操作系统命令注入漏洞，该漏洞源于外部输入数据构造操作系统可执行命令过程中，网络系统或产品未正确过滤其中的特殊字符、命令导致。攻击者可利用该漏洞执行非法操作系统命令。

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.accellion.com/products/fta/

2. Nagios XI 操作系统命令注入漏洞（CNNVD-202102-1136）

Nagios XI 是美国 Nagios 公司的一套 IT 基础设施监控解决方案。该方案支持对应用、服务、操作系统等进行监控和预警。

NagiosXI xi-5.7.5 中存在操作系统命令注入漏洞，该漏洞源于外部输入数据构造可执行命令过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞执行非法命令。

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.nagios.com/

3. 思科 Cisco AnyConnect Secure Mobility Client 数据伪造问题漏洞（CNNVD-202102-1301）

Cisco Anyconnect Secure Mobility Client 是美国思科（Cisco）公司的一款用于安全连接的 VPN 客户端软件。

Cisco AnyConnect Secure Mobility Client 中存在数据伪造问题漏洞，该漏洞源于网络系统或产品未充分验证数据的来源或真实性。攻击者可利用伪造的数据进行攻击。

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-anyconnect-dll-hijac-JrcTOQMC

二、接报漏洞情况

本周 CNNVD 接报漏洞 1493 个，其中信息技术产品漏洞（通用型漏洞）13 个，网络信息系统漏洞（事件型漏洞）1480 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	上海斗像信息科技有限公司	980
2	网神信息技术（北京）股份有限公司	429
3	北京天地和兴科技有限公司	30
4	山东华鲁科技发展股份有限公司	16
5	北京数字观星科技有限公司	13
6	任子行网络技术股份有限公司	8
7	北京圣博润高新技术股份有限公司	5
8	河南听潮盛世信息技术有限公司	5
9	北京威努特技术有限公司	3
10	山东云天安全技术有限公司	3
11	恒安嘉新（北京）科技股份公司	1
报送总计		1493

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 6 份。

序号	报送单位	预警总量
1	北京华云安信息技术有限公司	2

2	北京天融信网络安全技术有限公司	1
3	北京安天网络安全技术有限公司	1
4	北京华顺信安科技有限公司	1
5	内蒙古奥创科技有限公司	1
报送总计		6

信息安全漏洞周报

（2021 年 2月　　第 4 周）

CNNVD　　2020 年 2 月 28 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2021 年 2 月 22 日至 2021 年 2 月 28 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 243 个，与上周（255 个）相比减少了 4.71%。

接报漏洞情况

本周 CNNVD 接报漏洞 2484 个，其中信息技术产品漏洞（通用型漏洞）13 个，网络信息系统漏洞（事件型漏洞）2471 个。

重大漏洞预警

VMware 多个安全漏洞：包括 VMware vSphere Client 安全漏洞(CNNVD-202102-1566、CVE-2021-21972)、VMware ESXi 安全漏洞（CNNVD-202102-1560、CVE-2021-21974）。成功利用漏洞的攻击者可以在目标系统中远程执行恶意代码。vSphere Client 6.5、6.7、7.0，ESXi 6.5、6.7、7.0 等多个版本均受此漏洞影响。目前官方已在最新版本中修复了该漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞 243 个，漏洞新增数量有所下降。从厂商分布来看 IBM 公司新增漏洞最多，有 13 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 14.40%。新增漏洞中，超危漏洞 23 个，高危漏洞 63 个，中危漏洞 153 个，低危漏洞 4 个。相应修复率分别为 73.91%、77.78%、88.24% 和 100.00%。根据补丁信息统计，合计 205 个漏洞已有修复补丁发布，整体修复率为 84.36%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 243 个与上周（255 个）相比减少了 4.71%。

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，IBM 公司新增漏洞最多，有 13 个。各厂商漏洞数量分布如表 1 所示。

表 1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量（个）	所占比例
1	IBM	13	5.35%
2	思科	13	5.35%
3	Mozilla 基金会	13	5.35%
4	Micro Focus	6	2.47%
5	VMware	4	1.65%

本周国内厂商漏洞 17 个，联发科技公司漏洞数量最多，有 6 个。国内厂商漏洞整体修复率为 58.82%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 14.40%。漏洞类型统计如表 2 所示。

表 2 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	35	14.40%
2	命令注入	11	4.53%
3	缓冲区错误	10	4.12%
4	注入	7	2.88%
5	信任管理问题	7	2.88%
6	信息泄露	6	2.47%
7	路径遍历	5	2.06%
8	访问控制错误	5	2.06%
9	跨站请求伪造	5	2.06%
10	输入验证错误	4	1.65%
11	资源管理错误	4	1.65%
12	代码问题	3	1.23%
13	权限许可和访问控制问题	2	0.82%
14	操作系统命令注入	2	0.82%
15	SQL 注入	1	0.41%
16	代码注入	1	0.41%
17	数据伪造问题	1	0.41%
18	数字错误	1	0.41%
19	参数注入	1	0.41%
20	其他	129	53.09%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 23 个，高危漏洞 63 个，中危漏洞 153 个，低危漏洞 4 个。相应修复率分别为 73.91%、77.78%、88.24%和 100.00%。根据补丁信息统计，合计 205 个漏洞已有修复补丁发布，整体修复率为 84.36%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	23	17	73.91%
2	高危	63	49	77.78%
3	中危	153	135	88.24%
4	低危	4	4	100.00%
合计		243	205	84.36%

（四） 本周重要漏洞实例

本期重要漏洞实例如表 4 所示。

表 4 本期重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	其他	CNNVD-202102-1566	Vmware	Vmware vSphere Client 安全漏洞	是	超危
2	其他	CNNVD-202102-1515	Mozilla 基金会	Mozilla Firefox 安全漏洞	是	高危
3	其他	CNNVD-202102-1562	思科	Cisco NX-OS Software 安全漏洞	是	高危

1. VMware vSphere Client 安全漏洞（CNNVD-202102-1566）

VMware vSphere Client 是美国威睿（VMware）公司的一个应用软件，提供虚拟化管理。

VMware vSphere Client 存在一个安全漏洞，未授权的攻击者可

以通过开放443端口的服务器向vCenter Server发送精心构造的请求，从而在目标系统上远程执行恶意代码。以下产品和版本受到影响：vSphere Client 6.5、vSphere Client 6.7、vSphere Client 7.0、VMware Cloud Foundation（vCenter Server）3.x、VMware Cloud Foundation（vCenter Server）4.x。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.vmware.com/security/advisories/VMSA-2021-0002.html

2. Mozilla Firefox 安全漏洞（CNNVD-202102-1515）

Mozilla Firefox是美国Mozilla基金会的一款开源Web浏览器。

Mozilla Firefox 中存在安全漏洞。以下产品及版本受到影响：Firefox < 86

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.mozilla.org/en-US/security/advisories/mfsa2021-09/

3. Cisco NX-OS Software 安全漏洞（CNNVD-202102-1562）

Cisco NX-OS Software是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。

Cisco NX-OS Software 存在安全漏洞，该漏洞允许未经身份验证的远程攻击者，利用该漏洞在受影响的设备上造成拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSe

curityAdvisory/cisco-sa-nxos-ipv6-netstack-edXPGV7K

二、接报漏洞情况

本周 CNNVD 接报漏洞 2484 个，其中信息技术产品漏洞（通用型漏洞）13 个，网络信息系统漏洞（事件型漏洞）2471 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	上海斗像信息科技有限公司	1341
2	网神信息技术（北京）股份有限公司	721
3	山东新潮信息技术有限公司	62
4	西安四叶草信息技术有限公司	60
5	北京天地和兴科技有限公司	59
6	山东华鲁科技发展股份有限公司	31
7	西安交大捷普网络科技有限公司	30
8	山东云天安全技术有限公司	24
9	北京华云安信息技术有限公司	20
10	星云博创科技有限公司	20
11	杭州海康威视数字技术股份有限公司	17
12	北京数字观星科技有限公司	13
13	内蒙古奥创科技有限公司	12
14	任子行网络技术股份有限公司	12
15	深信服科技股份有限公司	11
16	天通高新集团有限公司	10
17	上海安识网络科技有限公司	9
18	北京圣博润高新技术股份有限公司	5

19	河南听潮盛世信息技术有限公司	5
20	中国电信集团系统集成有限责任公司网信安全业务部	4
21	安徽长泰信息安全服务有限公司	3
22	北京威努特技术有限公司	3
23	北京机沃科技有限公司	3
24	中国电信集团系统集成有限责任公司云计算安全与服务事业部	3
25	北京国舜科技股份有限公司	1
26	北京启明星辰信息安全技术有限公司	1
27	北京天融信网络安全技术有限公司	1
28	北京云测信息科技有限公司	1
29	恒安嘉新（北京）科技股份公司	1
30	北京山石网科信息技术有限公司	1
报送总计		2484

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 64 份。

序号	报送单位	预警总量
1	深信服科技股份有限公司	14
2	北京华云安信息技术有限公司	7
3	北京启明星辰信息安全技术有限公司	6
4	北京知道创宇信息技术股份有限公司	6
5	博智安全科技股份有限公司	4
6	内蒙古奥创科技有限公司	3

7	北京奇虎科技有限公司	3
8	网神信息技术（北京）股份有限公司	3
9	任子行网络技术股份有限公司	2
10	北京华顺信安科技有限公司	2
11	北京天融信网络安全技术有限公司	2
12	北京山石网科信息技术有限公司	2
13	新华三技术有限公司	2
14	杭州安恒信息技术股份有限公司	2
15	浪潮电子信息产业股份有限公司	2
16	内蒙古洞明科技有限公司	1
17	华为技术有限公司 未然实验室	1
18	远江盛邦(北京)网络安全科技股份有限公司	1
19	长扬科技（北京）有限公司	1
报送总计		64

四、重大漏洞预警

VMware 多个安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 VMware 多个安全漏洞情况的报送，其中包括 VMware vSphere Client 安全漏洞(CNNVD-202102-1566、CVE-2021-21972)、VMware ESXi 安全漏洞（CNNVD-202102-1560、CVE-2021-21974）。成功利用漏洞的攻击者可以在目标系统中远程执行恶意代码。vSphere Client 6.5、vSphere Client 6.7、vSphere Client 7.0、VMware Cloud Foundation（vCenter

Server）3.x、VMware Cloud Foundation（vCenter Server）4.x、ESXi 6.5、ESXi 6.7、ESXi 7.0、VMware Cloud Foundation (ESXi)3.X、VMware Cloud Foundation (ESXi)4.X 均受此漏洞影响。目前官方已在最新版本中修复了该漏洞，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

1、VMware vSphere Client 安全漏洞(CNNVD-202102-1566、CVE-2021-21972)：

VMware vSphere Client 是美国威睿（VMware）公司的一个应用软件，提供虚拟化管理。VMware vSphere Client 存在一个安全漏洞，未授权的攻击者可以通过开放 443 端口的服务器向 vCenter Server 发送精心构造的请求，从而在目标系统上远程执行恶意代码。

2、VMware ESXi 安全漏洞（CNNVD-202102-1560、CVE-2021-21974）：

VMware ESXi 是美国威睿（VMware）公司的一套可直接安装在物理服务器上的服务器虚拟化平台。VMware ESXi 存在一个安全漏洞，攻击者与 ESXi 处于同一网段且可以访问 427 端口时,可以通过向 427 端口发送恶意请求包触发 OpenSLP 服务中的堆溢出漏洞,最终造成远程代码执行。

.危害影响

成功利用漏洞的攻击者可以在目标系统中远程执行恶意代码。

vSphere Client 6.5、vSphere Client 6.7、vSphere Client 7.0、VMware Cloud Foundation（vCenter Server）3.x、VMware Cloud Foundation（vCenter Server）4.x、ESXi 6.5、ESXi 6.7、ESXi 7.0、VMware Cloud Foundation (ESXi)3.X、VMware Cloud Foundation (ESXi)4.X 均受此漏洞影响。

.修复建议

目前官方已在最新版本中修复了该漏洞，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.vmware.com/security/advisories/VMSA-2021-0002.html