北京师范大学网络信息安全通告

2020年 11 月报告

北京师范大学信息网络中心

2020 年 12 月

信息安全漏洞周报

（2020 年11月　第 1周）

CNNVD　　2020 年 11 月 08日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 11 月 02 日至 2020 年 11 月 08 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 361 个，与上周（265 个）相比增加了 36.23%。

接报漏洞情况

本周 CNNVD 接报漏洞 2011 个，其中信息技术产品漏洞（通用型漏洞）49 个，网络信息系统漏洞（事件型漏洞）1962 个。

重大漏洞　警

Linux kernel 缓冲区错误漏洞(CNNVD-202010-742、CVE-2020-27194)：成功利用漏洞的攻击者可以利用此漏洞在本地系统造成内核信息泄露或特权提升，进而控制目标服务器。Linux-5.7 - Linux-5.8.14、Ubuntu 20.10 均受此漏洞影响。目前，linux 官方已发布补丁修复了该漏洞，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 361 个，漏洞新增数量有所上升。从厂商分布来看 Cisco 公司新增漏洞最多，有 37 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 7.76%。新增漏洞中，超危漏洞 30 个，高危漏洞 119 个，中危漏洞 199 个，低危漏洞 13 个。相应修复率分别为 86.67%、90.76%、94.47%和 100.00%。根据补丁信息统计，合计 335 个漏洞已有修复补丁发布，整体修复率为 92.80%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 361 与上周（265 个）相比增多了 36.23%。

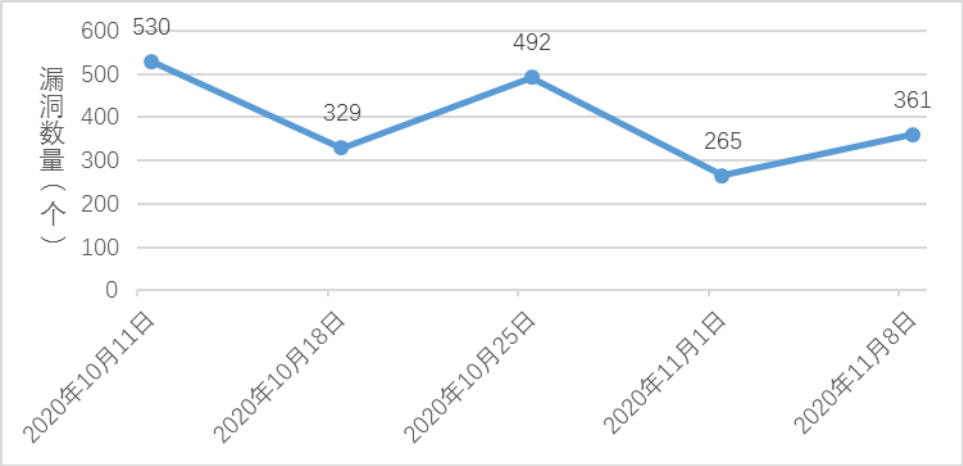

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Cisco 公司新增漏洞最多，有 37 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	Cisco	37	10.25%
2	Google	33	9.14%
3	Qualcomm	26	7.20%
4	Apple	25	6.93%
5	CloudBees	21	5.82%

本周国内厂商漏洞 15 个，Moxa 公司漏洞数量最多，有 3 个。国内厂商漏洞整体修复率为 66.67%。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 7.76%。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	28	7.76%
2	缓冲区错误	28	7.76%
3	授权问题	26	7.20%
4	输入验证错误	19	5.26%
5	资源管理错误	13	3.60%
6	代码问题	12	3.32%
7	信息泄露	9	2.49%
8	访问控制错误	9	2.49%
9	注入	7	1.94%
10	路径遍历	7	1.94%
11	跨站请求伪造	5	1.39%
12	权限许可和访问控制问题	2	0.55%
13	数据伪造问题	2	0.55%
14	加密问题	2	0.55%
15	SQL 注入	1	0.28%
16	命令注入	1	0.28%
17	操作系统命令注入	1	0.28%
18	后置链接	1	0.28%
19	安全特征问题	1	0.28%
20	竞争条件问题	1	0.28%
21	环境问题	1	0.28%

22	参数注入	1	0.28%
23	其他	183	50.69%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 30 个， 危漏洞 119 个，中危漏洞 199 个，低危漏洞 13 个。相应修复率分别为 86.67%、90.76%、94.47%和 100.00%。根据补丁信息统计，合计 335 个漏洞已有修复补丁发布，整体修复率为 92.80%。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	30	26	86.67%
2	危	119	108	90.76%
3	中危	199	188	94.47%
4	低危	13	13	100.00%
合计		361	335	92.80%

（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	缓冲区错误	CNNVD-202011-168	Google	Google Chrome for Windows 缓冲区错误漏洞	是	超危
2	资源管理错误	CNNVD-202011-184	Adobe	Adobe Reader 资源管理错误漏洞	是	危
3	其他	CNNVD-202011-287	Cisco	Cisco SD-WAN vEdge 安全漏洞	是	危

1. Google Chrome for Windows 缓冲区错误漏洞（CNNVD-202011-168）

Google Chrome for Windows 是美国谷歌（Google）公司的一款基于 Windows 平台的 Web 浏览器。

Windows Google Chrome 86.0.4240.183 之前版本存在缓冲区错误漏洞，该漏洞源于浏览器 UI 中的堆缓冲区溢出危害渲染器进程，攻击者可通过精心制作的 HTML 页面执行沙箱转义。

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/2020/11/stable-channel-update-for-desktop.html

2. Adobe Reader 资源管理错误漏洞（CNNVD-202011-184）

Adobe Reader 是美国奥多比（Adobe）公司的一套 PDF 文档阅读软件。

Adobe Acrobat Reader 中存在资源管理错误漏洞，该漏洞源于网络系统或产品在内存上执行操作时，未正确　证数据边界，导致向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://helpx.adobe.com/security/products/acrobat/apsb20-67.html

3. Cisco SD-WAN vEdge 安全漏洞（CNNVD-202011-287）

Cisco SD-WAN vEdge 是美国思科（Cisco）公司的是一款路由器。该设备可为思科 SD-WAN 解决方案提供基本 WAN，安全性和多云功能。

Cisco SD-WAN 中存在安全漏洞。攻击者可以通过 Cisco SD-WAN

vEdge 的 CLI 文件创建触发致命错误，进而触发拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vsoln-arbfile-gtsEYxns

二、接报漏洞情况

本周 CNNVD 接报漏洞 2011 个，其中信息技术产品漏洞（通用型漏洞）49 个，网络信息系统漏洞（事件型漏洞）1962 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	上海斗象信息科技有限公司	1035
2	网神信息技术（北京）股份有限公司	442
3	北京奇虎科技有限公司	208
4	北京山石网科信息技术有限公司	114
5	长春嘉诚信息技术股份有限公司	68
6	山东新潮信息技术有限公司	30
7	中新网络信息安全股份有限公司	29
8	新华三技术有限公司	27
9	杭州迪普科技股份有限公司	20
10	山东华　科技发展股份有限公司	14
11	上海安识网络科技有限公司	4
12	中兴通讯	4
13	杭州海康威视数字技术股份有限公司	4
14	上海安几科技有限公司	3
15	北京天融信网络安全技术有限公司	2

16	广东东福信息技术有限公司	2
17	西安交大捷普网络科技有限公司	2
18	亚信科技（成都）有限公司	2
19	国防科技大学	1
报送总计		2011

三、接报漏洞　警情况

本周 CNNVD 接报漏洞　警 72 个。

	报送单位	警总量
1	杭州迪普科技股份有限公司	15
2	中国电信股份有限公司网络安全产品运营中心	15
3	北京奇虎科技有限公司	7
4	北京华顺信安科技有限公司	6
5	网神信息技术（北京）股份有限公司	5
6	深信服科技股份有限公司	5
7	浪潮电子信息产业股份有限公司	4
8	北京启明星辰信息安全技术有限公司	3
9	北京知道创宇信息技术股份有限公司	3
10	北京华云安信息技术有限公司	3
11	北京天融信网络安全技术有限公司	2
12	北京神州绿盟科技有限公司	1
13	新华三技术有限公司	1
14	杭州安恒信息技术股份有限公司	1
15	北京安帝科技有限公司	1

报送总计	72

四、重大漏洞预警

CNNVD 关于 Linux kernel 缓冲区错误漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于 Linux kernel 缓冲区错误漏洞(CNNVD-202010-742、CVE-2020-27194)情况的报送。成功利用漏洞的攻击者可以利用此漏洞在本地系统造成内核信息泄露或特权提升，进而控制目标服务器。Linux-5.7 - Linux-5.8.14、Ubuntu 20.10 均受此漏洞影响。目前，linux 官方已发布补丁修复了该漏洞，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

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。Linux kernel 5.8.15 之前版本存在安全漏洞，该漏洞是由于 eBPF 证程序中进行 or 操作时未正确计算寄存器范围，进而引发越界读取和写入，导致攻击者可以利用此漏洞造成内核信息泄露或特权提升。

.危害影响

成功利用漏洞的攻击者可以利用此漏洞在本地系统造成内核信息泄露或特权提升，进而控制目标服务器。Linux-5.7 - Linux-5.8.14、Ubuntu 20.10 均受此漏洞影响。

.修复建议

目前，linux 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://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.8.15

信息安全漏洞周报

（2020 年1 1 月　　第 2 周 ）

CNNVD　　**2020 年 11 月 17 日**

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 11 月 9 日至 2020 年 11 月 15 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 387 个，与上周（361 个）相比增加了 7.20%。

接报漏洞情况

本周 CNNVD 接报漏洞 2445 个，其中信息技术产品漏洞（通用型漏洞）165 个，网络信息系统漏洞（事件型漏洞）2280 个。

重大漏洞预警

近日，微软官方发布了多个安全漏洞的公告，包括 Windows 权限提升漏洞（CNNVD-202010-1673）、Windows NFS 远程代码执行漏洞（CNNVD-202011-783）、Windows Exchange Server 远程代码执行漏洞（CNNVD-202011-755）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。

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 387 个，漏洞新增数量有所上升。从厂商分布来看 Microsoft 公司新增漏洞最多，有 111 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 6.98%。新增漏洞中，超危漏洞 13 个，高危漏洞 146 个，中危漏洞 220 个，低危漏洞 8 个。相应修复率分别为 92.31%、92.47%、90.00%和 87.50%。根据补丁信息统计，合计 352 个漏洞已有修复补丁发布，整体修复率为 90.96%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 387 个，与上周（361 个）相比增多了 7.20%。

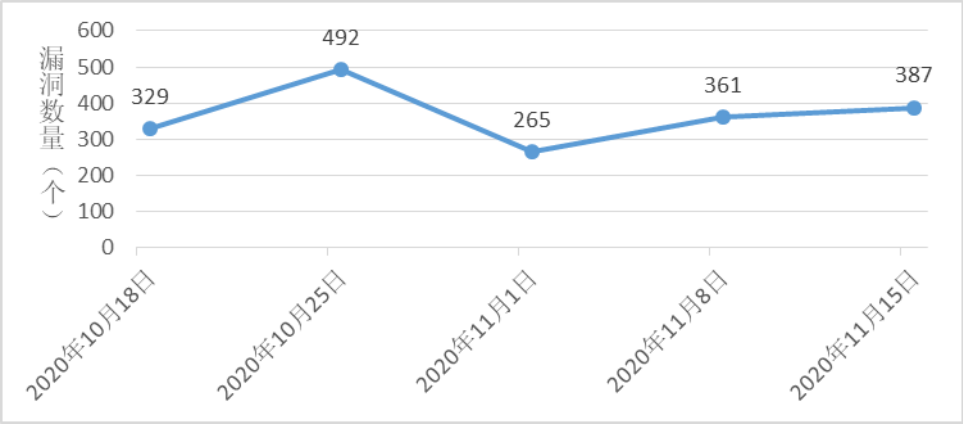

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Microsoft 公司新增漏洞最多，有 111 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	Microsoft	111	28.68%
2	Intel	45	11.63%
3	Apple	28	7.24%
4	IBM	20	5.17%
5	SAP	17	4.39%

本周国内厂商漏洞 3 个，Huawei 公司漏洞数量最多，有 3 个。国内厂商漏洞整体修复率为 100.00%。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，跨站脚本类的安全漏洞占比最大，达到 6.98%。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	27	6.98%
2	访问控制错误	16	4.13%
3	资源管理错误	12	3.10%
4	代码问题	11	2.84%
5	信息泄露	10	2.58%
6	缓冲区错误	8	2.07%
7	SQL 注入	7	1.81%
8	授权问题	6	1.55%
9	配置错误	5	1.29%
10	跨站请求伪造	4	1.03%
11	输入验证错误	3	0.78%
12	注入	3	0.78%
13	路径遍历	3	0.78%
14	默认配置问题	3	0.78%
15	权限许可和访问控制问题	2	0.52%
16	加密问题	1	0.26%
17	命令注入	1	0.26%
18	代码注入	1	0.26%
19	日志信息泄露	1	0.26%
20	其他	263	67.96%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 13 个，高危漏洞 146 个，中危漏洞 220 个，低危漏洞 8 个。相应修复率分别为 92.31%、92.47%、90.00%和 87.50%。根据补丁信息统计，合计 352 个漏洞已有修复补丁发布，整体修复率为 90.96%。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	13	12	92.31%
2	高危	146	135	92.47%
3	中危	220	198	90.00%
4	低危	8	7	87.50%
合计		387	352	90.96%

（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	访问控制错误	CNNVD-202011-1336	Citrix Systems	Citrix Systems SD-WAN Center 访问控制错误漏洞	是	超危
2	代码问题	CNNVD-202011-842	Schneider Electric	Schneider Electric EcoStruxure Control Expert 代码问题漏洞	是	高危
3	缓冲区错误	CNNVD-202011-853	Intel	Intel Stratix FPGA firmware provided Intel Quartus Prime Pro software 缓冲区错误漏洞	是	高危

1. Citrix Systems SD-WAN Center 访问控制错误漏洞（CNNVD-202011-1336）

Citrix Systems SD-WAN Center 是美国思杰系统（Citrix Systems）公司的一套集中管理系统。该系统主要用于配置、监控和分析 WAN 上的所有 Citrix SD-WAN 设备。

Citrix SD-WAN 存在访问控制错误漏洞，该漏洞允许一个未经身份验证的攻击与网络访问 SD-WAN 中心作为 root 用户执行任意代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.citrix.com/article/CTX285061

2. Schneider Electric EcoStruxure Control Expert 代码问题漏洞（CNNVD-202011-842）

Schneider Electric EcoStruxure Control Expert（前称 Unity Pro）是法国施耐德电气（Schneider Electric）公司的一套用于 Schneider Electric 逻辑控制器产品的编程软件。

EcoStruxure Control Expert 的 PLC 模拟器中存在代码问题漏洞，该漏洞源于当通过 Modbus 收到一个特别制作的请求时，会导致 EcoStruxure 控制专家软件中的 PLC 模拟器崩溃。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.se.com/ww/en/download/document/SEVD-2020-315-07/

3. Intel Stratix FPGA firmware provided Intel Quartus Prime Pro software 缓冲区错误漏洞（CNNVD-202011-853）

Intel PAC with Arria 10 GX FPGA 是美国英特尔（Intel）公

司的一款采用英特尔 Arria 10 GX FPGA（现场可编程门阵列）的可编程加速卡。

Intel(R) Stratix(R) 10 FPGA firmware provided Intel(R) Quartus(R) Prime Pro software 20.2 之前版本存在缓冲区错误漏洞，该漏洞允许未经身份验证的用户启用升级特权和信息披露的物理访问。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00388.html

二、接报漏洞情况

本周 CNNVD 接报漏洞 2445 个，其中信息技术产品漏洞（通用型漏洞）165 个，网络信息系统漏洞（事件型漏洞）2280 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1.	上海斗象信息科技有限公司	957
2.	网神信息技术（北京）股份有限公司	608
3.	北京山石网科信息技术有限公司	328
4.	北京微步在线科技有限公司	114
5.	长春嘉诚信息技术股份有限公司	70
6.	北京启明星辰信息安全技术有限公司	59
7.	中新网络信息安全股份有限公司	57
8.	北京华云安信息技术有限公司	43
9.	山东华鲁科技发展股份有限公司	31

10.	北京顶象技术有限公司 洞见安全实验室	26
11.	内蒙古奥创科技有限公司	22
12.	北京天地和兴科技有限公司	15
13.	北京锦龙信安科技有限公司	14
14.	中国电信集团系统集成有限责任公司	14
15.	杭州迪普科技股份有限公司	12
16.	北京数字观星科技有限公司	10
17.	山东云天安全技术有限公司	10
18.	深圳市魔方安全科技有限公司	10
19.	北京梆梆安全科技有限公司	7
20.	北京邮电大学	6
21.	北京威努特技术有限公司	4
22.	深信服科技股份有限公司	4
23.	中兴通讯	4
24.	亚信科技（成都）有限公司	4
25.	北京天融信网络安全技术有限公司	3
26.	北京中测安华科技有限公司	3
27.	北京智游网安科技有限公司	2
28.	美国印第安纳大学伯明顿分校，中国科学院信息工程研究所	1
29.	长亭科技	1
30.	中国信息安全测评中心	1
31.	个人提交者	5
报送总计		2445

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 36 个。

	报送单位	预警总量
1	杭州迪普科技股份有限公司	15
2	北京奇虎科技有限公司	4
3	北京启明星辰信息安全技术有限公司	3
4	北京华云安信息技术有限公司	2
5	北京神州绿盟科技有限公司	2
6	北京知道创宇信息技术股份有限公司	2
7	深信服科技股份有限公司	2
8	北京安天网络安全技术有限公司	1
9	北京天融信网络安全技术有限公司	1
10	北京中测安华科技有限公司	1
11	网神信息技术（北京）股份有限公司	1
12	新华三技术有限公司	1
13	远江盛邦（北京）网络安全科技股份有限公司	1
报送总计		36

四、重大漏洞预警

CNNVD 关于微软多个安全漏洞的通报

近日，微软官方发布了多个安全漏洞的公告，包括 Windows 权限提升漏洞（CNNVD-202010-1673、CVE-2020-17087）、Windows NFS 远程代码执行漏洞（CNNVD-202011-783、CVE-2020-17051）、Windows

Exchange Server 远程代码执行漏洞（CNNVD-202011-755、CVE-2020-17084）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。

（一） 漏洞介绍

2020 年 11 月 11 日，微软发布了 2020 年 11 月份安全更新，共 112 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、IE/Edge 浏览器、Office 组件及 Web Apps、ChakraCore、Exchange 服务器、.Net 框架、Azure DevOps、Windows Defender、Visual Studio 等多个 Windows 平台下应用软件和组件。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，其中部分重要漏洞详情如下：

1、Windows cng.sys 权限提升漏洞（CNNVD-202010-1673、CVE-2020-17087）

漏洞简介：Windows Kernel 中存在一个本地权限提升漏洞，未授权的攻击者通过 诱使用户运行恶意的二进制程序 ，最终造成 权限提升 。

2、Windows NFS 远程代码执行漏洞（CNNVD-202011-783、CVE-2020-17051）

漏洞简介：Windows NFS 是一种网络文件系统，用户可以通过 NFS 访问网络上的文件并将它们像本地文件一样操作。攻击者可以利用此漏洞来访问系统，并远程执行恶意代码。

3、Windows Exchange Server 远程代码执行漏洞（CNNVD-202011-755、CVE-2020-17084）

漏洞简介：Windows Exchange Server 中存在一个远程代码执行漏洞，未授权的远程攻击者通过向 Exchage 服务器发送特制的请求包来进行漏洞利用，利用成功后便可获得服务器完整控制权限。

4、Windows Hyper-V 验证绕过漏洞（CNNVD-202011-792、CVE-2020-17040）

漏洞简介：未授权的远程攻击通过向 Hyper-V 服务器发送特制的请求包来进行漏洞利用，利用成功后便可绕过 Hyper-V 现有的部分安全特性。

由于此次更新，微软并没有透露太多漏洞详情，请用户自行到官方网站查询，官方地址：

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

（二）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

（2020 年11月　第3周）

CNNVD　　2020 年 11 月 24 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 11 月 16 日至 2020 年 11 月 22 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 312 个，与上周（387 个）相比减少了 19.38%。

接报漏洞情况

本周 CNNVD 接报漏洞 2509 个，其中信息技术产品漏洞（通用型漏洞）47 个，网络信息系统漏洞（事件型漏洞）2462 个。

重大漏洞预警

Drupal 安全漏洞（CNNVD-202011-1698、CVE-2020-13671）：成功利用漏洞的远程攻击者可能获取目标系统或网站的管理权限，执行恶意代码。Drupal Core 7、8.8、8.9、9.0 各分支版本均受此漏洞影响。目前，Drupal 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Drupal Core 产品版本，如受影响，请及时采取修补措施。

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 312 个，漏洞新增数量有所下降。从厂商分布来看 Google 公司新增漏洞最多，有 25 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 11.86%。新增漏洞中，超危漏洞 30 个，高危漏洞 87 个，中危漏洞 190 个，低危漏洞 5 个。相应修复率分别为 73.33%、90.80%、87.37%和 100.00%。根据补丁信息统计，合计 272 个漏洞已有修复补丁发布，整体修复率为 87.18%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 312 与上周（387 个）相比减少了 19.38%。

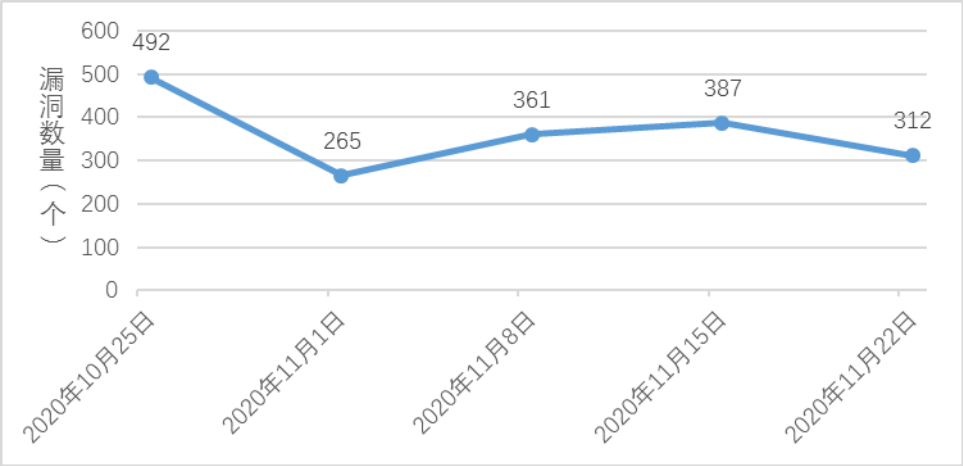

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Google 公司新增漏洞最多，有 25 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	Google	25	8.01%
2	Cisco	22	7.05%
3	Mozilla 基金会	20	6.41%
4	JetBrains	14	4.49%
5	Trend Micro	12	3.85%

本周国内厂商漏洞 9 个，TP-Link 公司漏洞数量最多，有 3 个。国内厂商漏洞整体修复率为 88.89%。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 11.86%。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	37	11.86%
2	缓冲区错误	25	8.01%
3	访问控制错误	15	4.81%
4	输入验证错误	13	4.17%
5	代码问题	10	3.21%
6	SQL 注入	10	3.21%
7	授权问题	9	2.88%
8	信息泄露	5	1.60%
9	注入	4	1.28%
10	权限许可和访问控制问题	4	1.28%
11	资源管理错误	3	0.96%
12	加密问题	3	0.96%
13	操作系统命令注入	3	0.96%
14	路径遍历	2	0.64%
15	命令注入	2	0.64%
16	信任管理问题	2	0.64%
17	代码注入	1	0.32%
18	参数注入	1	0.32%
19	其他	162	51.92%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 30 个， 危漏洞 87 个，中危漏洞 190 个，低危漏洞 5 个。相应修复率分别为 73.33%、90.80%、87.37%和 100.00%。根据补丁信息统计，合计 272 个漏洞已有修复补丁发布，整体修复率为 87.18%。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	30	22	73.33%
2	危	87	79	90.80%
3	中危	190	166	87.37%
4	低危	5	5	100.00%
合计		312	272	87.18%

（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-202011-1762	VMware	VMware ESXi 安全漏洞	是	超危
2	缓冲区错误	CNNVD-202011-1597	Google	Google Chrome 缓冲区错误漏洞	是	危
3	缓冲区错误	CNNVD-202011-1500	Mozilla 基金会	Mozilla Firefox ESR 缓冲区错误漏洞	是	危

1. VMware ESXi 安全漏洞（CNNVD-202011-1762）

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 存在安全漏洞，该漏洞源于 XHCI USB 控制器中包

含无后使用漏洞。在虚拟机上具有本地管理权限的恶意参与者可能会利用这个问　来执行在主机上运行的虚拟机的 VMX 进程的代码。以下产品及版本受到影响：VMware ESXi 7.0 ESXi70U1b-17168206 之前版本，6.7 ESXi670-202011101-SG 之前版本，6.5 ESXi650-202011301-SG 之前版本，Workstation 15.x 系列 15.5.7 之前版本，Fusion 11.x 系列 11.5.7 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.vmware.com/security/advisories/VMSA-2020-0026.html

2. Google Chrome 缓冲区错误漏洞（CNNVD-202011-1597）

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

Google chrome 87.0.4280.66 之前版本存在缓冲区错误漏洞，该漏洞源于 WebRTC 中的堆缓冲区溢出导致。

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/2020/11/stable-channel-update-for-desktop_17.html

3. Mozilla Firefox ESR 缓冲区错误漏洞（CNNVD-202011-1500）

Mozilla Firefox ESR 是美国 Mozilla 基金会的 Firefox(Web 浏览器)的一个延长支持版本。

Firefox 83.0 之前版本存在缓冲区错误漏洞，攻击者可利用该漏洞来运行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.mozilla.org/en-US/security/advisories/mfsa2020-50/

二、接报漏洞情况

本周 CNNVD 接报漏洞 2509 个，其中信息技术产品漏洞（通用型漏洞）47 个，网络信息系统漏洞（事件型漏洞）2462 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1.	上海斗象信息科技有限公司	1639
2.	网神信息技术（北京）股份有限公司	447
3.	长春嘉诚信息技术股份有限公司	224
4.	西安四叶草信息技术有限公司	59
5.	北京天地和兴科技有限公司	30
6.	北京山石网科信息技术有限公司	25
7.	星云博创科技有限公司	19
8.	杭州　安科技有限公司	13
9.	新华三技术有限公司	11
10.	北京数字观星科技有限公司	10
11.	北京邮电大学	8
12.	山东云天安全技术有限公司	8
13.	信息系统安全技术重点实　室	4
14.	北京安华金和科技有限公司	3
15.	亚信科技（成都）有限公司	2
16.	北京天融信网络安全技术有限公司	2
17.	个人	2

18.	信息工程大学	1
19.	北京智游网安科技有限公司	1
20.	美国印第安纳大学伯明　分校，中国科学院信息工程研究所	1
报送总计		2509

三、接报漏洞预警情况

本周 CNNVD 接报漏洞　警 59 个。

	报送单位	警总量
1	杭州迪普科技股份有限公司	15
2	北京华云安信息技术有限公司	9
3	北京华顺信安科技有限公司	5
4	北京知道创宇信息技术股份有限公司	5
5	深信服科技股份有限公司	4
6	北京启明星辰信息安全技术有限公司	4
7	北京奇虎科技有限公司	4
8	北京神州绿盟科技有限公司	3
9	北京山石网科信息技术有限公司	3
10	北京中测安华科技有限公司	2
11	北京天融信网络安全技术有限公司	1
12	新华三技术有限公司	1
13	浪潮电子信息产业股份有限公司	1
14	上海斗像信息科技有限公司	1
15	杭州安恒信息技术股份有限公司	1
报送总计		36

四、重大漏洞预警

CNNVD 关于 Drupal 安全漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于 Drupal 安全漏洞（CNNVD-202011-1698、CVE-2020-13671）情况的报送。成功利用漏洞的远程攻击者可能获取目标系统或网站的管理权限，执行恶意代码。Drupal Core 7、8.8、8.9、9.0 各分支版本均受此漏洞影响。目前，Drupal 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Drupal Core 产品版本，如受影响，请及时采取修补措施。

.漏洞介绍

Drupal 是 Drupal 社区的一套使用 PHP 语言开发的开源内容管理系统。

Drupal Core 存在安全漏洞，由于 Drupal Core 未正确处理上传文件中的某些文件名，可能导致文件会被错误地解析为其他 MIME 类型，未授权的远程攻击者可通过上传特定文件名的恶意文件利用漏洞执行代码。

.危害影响

成功利用该漏洞的远程攻击者，可获取目标系统或网站的管理权限，执行恶意代码。以下等版本均受此漏洞影响：

Drupal < 7.7.4

Drupal < 8.8.11

Drupal < 8.9.9

Drupal < 9.0.8

注：官方已经停止维护 8.8.x 之前的 Drupal 8 版本。

.修复建议

目前，Drupal 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Drupal Core 产品版本，如受影响，请及时采取修补措施。漏洞修补措施如下：

Drupal 9.0 系列用户，建议更新至 Drupal 9.0.8 版本，链接为 https://www.drupal.org/project/drupal/releases/9.0.8。

Drupal 8.9 系列用户，建议更新至 Drupal 8.9.9 版本，链接为 https://www.drupal.org/project/drupal/releases/8.9.9。

Drupal 8.8 系列用户，建议更新至 Drupal 8.8.11 版本，链接为 https://www.drupal.org/project/drupal/releases/8.8.11。

Drupal 7 系列用户，建议更新至 Drupal 7.74，链接为 https://www.drupal.org/project/drupal/releases/7.74。

信息安全漏洞周报

（2020 年11月　第4周）

CNNVD　　2020 年 12 月 01 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 11 月 23 日至 2020 年 11 月 29 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 181 个，与上周（312 个）相比减少了 41.99%。

接报漏洞情况

本周 CNNVD 接报漏洞 1658 个，其中信息技术产品漏洞（通用型漏洞）92 个，网络信息系统漏洞（事件型漏洞）1566 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 181 个，漏洞新增数量有所下降。从厂商分布来看 Linux 基金会公司新增漏洞最多，有 10 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 10.50%。新增漏洞中，超危漏洞 23 个，高危漏洞 44 个，中危漏洞 111 个，低危漏洞 3 个。相应修复率分别为 91.30%、95.45%、85.59%和 100.00%。根据补丁信息统计，合计 161 个漏洞已有修复补丁发布，整体修复率为 88.95%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 181 与上周（312 个）相比减少了 41.99%。

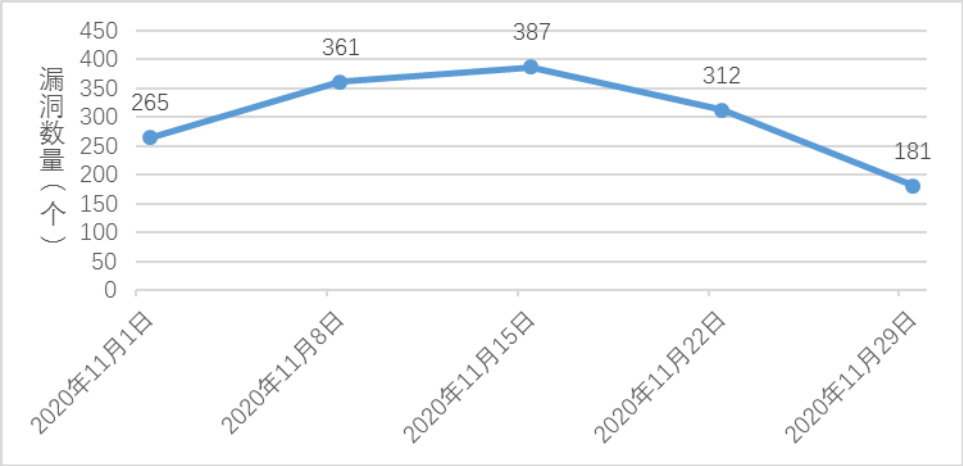

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Linux 基金会公司新增漏洞最多，有 10 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	Linux 基金会	10	5.52%
2	IBM	7	3.87%
3	Red Hat	5	2.76%
4	Rockwell Automation	3	1.66%
5	cPanel	3	1.66%

本周国内厂商漏洞 29 个，中国深圳西迪特公司漏洞数量最多，有 10 个。国内厂商漏洞整体修复率为 100.00%。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，跨站脚本类的安全漏洞占比最大，达到 10.50%。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	19	10.50%
2	输入验证错误	14	7.73%
3	缓冲区错误	13	7.18%
4	授权问题	7	3.87%
5	注入	7	3.87%
6	权限许可和访问控制问题	6	3.31%
7	代码问题	5	2.76%
8	路径遍历	5	2.76%
9	跨站请求伪造	5	2.76%
10	SQL 注入	4	2.21%
11	命令注入	4	2.21%
12	信任管理问题	4	2.21%
13	信息泄露	3	1.66%
14	访问控制错误	2	1.10%
15	资源管理错误	1	0.55%
16	加密问题	1	0.55%
17	其他	81	44.75%

（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 44 个，中危漏洞 111 个，低危漏洞 3 个。相应修复率分别为 91.30%、95.45%、85.59%和 100.00%。根据补丁信息统计，合计 161 个漏洞已有修复补丁发布，整体修复率为 88.95%。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	21	91.30%
2	高危	44	42	95.45%
3	中危	111	95	85.59%
4	低危	3	3	100.00%
合计		181	161	88.95%

（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	输入验证错误	CNNVD-202011-1855	Apache 基金会	Apache Unomi 输入验证错误漏洞	是	超危
2	权限许可和访问控制问题	CNNVD-202011-1793	Linux 基金会	Linux kernel 权限许可和访问控制问题漏洞	是	高危
3	跨站请求伪造	CNNVD-202011-1856	Fastweb	Fastweb FASTGate 跨站请求伪造漏洞	是	高危

1. Apache Unomi 输入验证错误漏洞（CNNVD-202011-1855）

Apache Unomi 是美国阿帕奇软件（Apache Software）基金会的一套开源的客户数据平台。该平台主要使用 Java 语言编写。

Apache Unomi 1.5.2 之前版本存在安全漏洞，该漏洞源于可以

将恶意的 OGNL 或 MVEL 脚本注入/context.json 公共端点。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

http://unomi.apache.org./security/cve-2020-13942.txt

2. Linux kernel 权限许可和访问控制问题漏洞（CNNVD-202011-1793）

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 5.8 之前版本存在安全漏洞，该漏洞源于 Use-after-free 漏洞允许本地用户通过不当访问某个错误字段来获得特权或导致拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://lkml.org/lkml/2020/6/7/379

3. Fastweb FASTGate 跨站请求伪造漏洞（CNNVD-202011-1856）

Fastweb FASTGate 是意大利 Fastweb 公司的一款调制解调器。

Fastweb FASTGate GPON FGA2130FWB 2020-05-26 版本及之前版本存在跨站请求伪造漏洞，该漏洞允许 CSRF 通过路由器管理 web 面板，从而使攻击者可利用该漏洞能够执行管理操作，比如修改配置。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://members.backbox.org/fastgate-gpon-cross-site-request-forgery/

二、接报漏洞情况

本周 CNNVD 接报漏洞 1658 个，其中信息技术产品漏洞（通用型

漏洞）92 个，网络信息系统漏洞（事件型漏洞）1566 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1.	上海斗象信息科技有限公司	954
2.	网神信息技术（北京）股份有限公司	239
3.	北京微步在线科技有限公司	83
4.	内蒙古奥创科技有限公司	73
5.	北京天地和兴科技有限公司	70
6.	山东华鲁科技发展股份有限公司	40
7.	山东新潮信息技术有限公司	30
8.	中国电子科技网络信息安全有限公司	22
9.	广州锦行网络科技有限公司	20
10.	亚信科技（成都）有限公司	19
11.	杭州海康威视数字技术股份有限公司	18
12.	浙江大华技术股份有限公司	16
13.	山东云天安全技术有限公司	13
14.	新华三技术有限公司	12
15.	北京数字观星科技有限公司	10
16.	北京安华金和科技有限公司	7
17.	北京山石网科信息技术有限公司	7
18.	绿盟科技集团股份有限公司安全研究部	5
19.	北京华云安信息技术有限公司	4
20.	国防科技大学	3
21.	北京中测安华科技有限公司	2

22.	北京天融信网络安全技术有限公司	2
23.	北京威努特技术有限公司	2
24.	广东东福信息技术有限公司	2
25.	广州竞远安全技术股份有限公司	2
26.	北京安信天行科技有限公司	1
27.	北京智游网安科技有限公司	1
28.	四川大学网络空间安全学院、北京未来安全信息技术有限公司	1
报送总计		1658

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 46 个。

	报送单位	预警总量
1	杭州迪普科技股份有限公司	15
2	深圳开源互联网安全技术有限公司	12
3	北京知道创宇信息技术股份有限公司	4
4	北京华云安信息技术有限公司	3
5	深信服科技股份有限公司	3
6	北京天融信网络安全技术有限公司	2
7	北京神州绿盟科技有限公司	1
8	新华三技术有限公司	1
9	杭州安恒信息技术股份有限公司	1
10	远江盛邦(北京)网络安全科技股份有限公司	1
11	内蒙古洞明科技有限公司	1
12	北京奇虎科技有限公司	1

13	北京中测安华科技有限公司	1
报送总计		46