国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 03 月 02 日-2020 年 03 月 08 日　　2020 年第 10 期

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 554 个，其中高危漏洞 197 个、中危漏洞 271 个、低危漏洞 86 个。漏洞平均分值为 6.08。本周收录的漏洞中，涉及 0day 漏洞 184 个（占 33%），其中互联网上出现“Tenda N301 拒绝服务漏洞、Comtrend VR-3033 命令注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2227 个，与上周（2413 个）环比减少 7%。

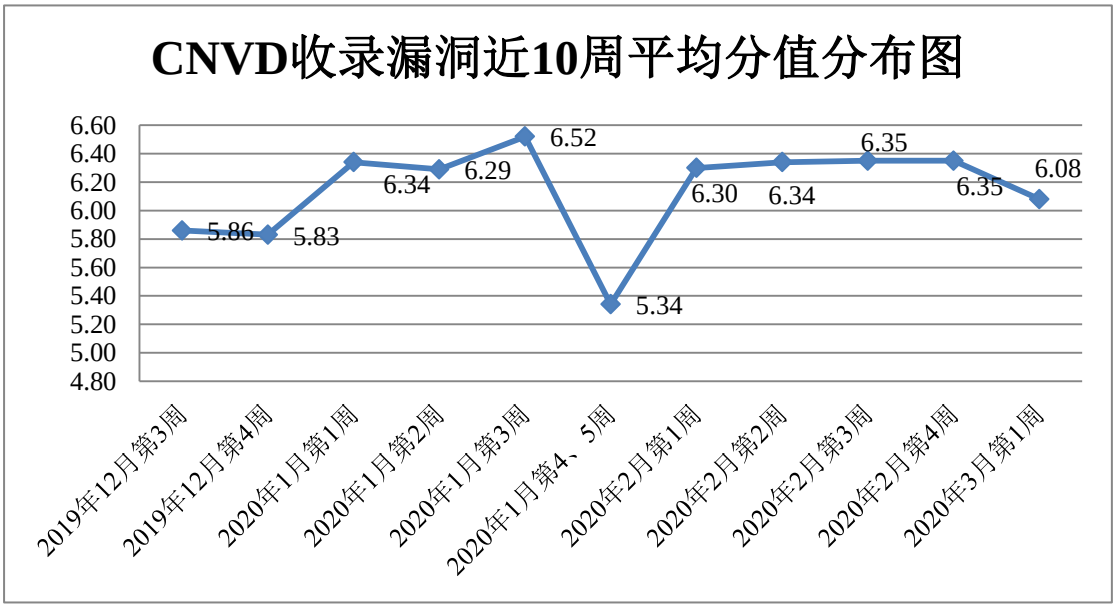

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 29 起，向基础电信企业通报漏洞事件 4 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞

事件 259 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 22 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 16 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

阿里巴巴网络技术有限公司、台安科技（无锡）有限公司、昆明云涛科技有限公司、酷溜网(北京)文化传媒有限公司、海南赞赞网络科技有限公司、台湾永宏电机股份有限公司、桂林天生智创信息技术有限公司、山西先启科技有限公司、深圳市迪元素科技有限公司、若无（上海）信息科技有限公司、湖北淘码千维信息科技有限公司、北京天生创想信息技术有限公司、福建多多云科技有限公司、深圳市吉祥腾达科技有限公司、杭州恒生数字设备科技有限公司、北京国炬信息技术有限公司、江苏金智教育信息股份有限公司、南京南软科技有限公司、上海驿氪信息科技有限公司、福建福昕软件开发股份有限公司、深圳雅科网络科技有限公司、用友网络科技股份有限公司、济南点创网络科技有限公司、北京珑大钜商科技有限公司、海南易而优科技有限公司、西安超越软件有限公司、厦门易商网络科技有限公司、北京博乐虎科技有限公司、营口爱思达计算机信息网络有限公司、圆梦云科技有限公司、中国中铁四局集团有限公司、北京辰信领创信息技术有限公司、南充市老虎云网络技术有限公司、珠海金山办公软件有限公司、开平市联科网络科技有限公司、神玥软件科技股份有限公司、乐清翰珂网络公司、合肥天寻信息科技有限公司、上海市民信箱信息服务有限公司、北京良精志诚科技有限责任公司、洛阳云业信息科技有限公司、怀化第五元素网络信息有限公司、深圳市科图自动化新技术应用公司、湖南壹拾捌号网络技术有限公司、深圳太乐文化科技有限公司、杭州神话信息技术有限公司、北京椒图科技有限公司、长沙友点软件科技有限公司、北京金山安全管理系统技术有限公司、上海彩圣信息科技有限公司、沈阳点动科技有限公司、上海秀可视科技有限公司、北京三快科技有限公司、武汉类森科技有限公司、无忧网络、邯郸爱情帮你办、睿谷信息管理系统、海洋 CMS、E 客开发团队、5iSNS 实验室、Guojiz、CONQUEST DICOM SERVER、MyuCMS、SemCms 和 JPress。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、北京天融信网络安全技术有限公司、华为技术有限公司、恒安嘉新(北京)科技股份公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。远江盛邦（北京）网络安全科技股份有限公司、国瑞数码零点实验室、北京华云安信息技术有限公司、山石网科通信技术股份有限公司、长春嘉诚信息技术股份有限公司、南京众智维信息科技有限公司、河南灵创电子科技有限公司、北京圣博润高新技术股份有限公司、杭州迪普科技股份有限公司、

山东云天安全技术有限公司、上海观安信息技术股份有限公司、银行卡检测中心、新疆海狼科技有限公司、北京智游网安科技有限公司、广州万方计算机科技有限公司及其他个人白帽子向 CNVD 提交了 2227 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 1195 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
斗象科技（漏洞盒子）	502	502
奇安信网神（补天平台）	398	398
上海交大	295	295
哈尔滨安天科技集团股份有限公司	201	0
北京天融信网络安全技术有限公司	125	11
华为技术有限公司	124	0
恒安嘉新(北京)科技股份公司	94	0
新华三技术有限公司	80	0
北京启明星辰信息安全技术有限公司	66	14
北京神州绿盟科技有限公司	38	2
深信服科技股份有限公司	5	5
中新网络信息安全股份有限公司	5	5
北京知道创宇信息技术股份有限公司	4	0
南京铱迅信息技术股份有限公司	3	3
南京联成科技发展股份有限公司	2	2
远江盛邦（北京）网络安全科技股份有限公司	109	109
国瑞数码零点实验室	108	108

北京华云安信息技术有限公司	87	87
山石网科通信技术股份有限公司	65	65
长春嘉诚信息技术股份有限公司	42	42
南京众智维信息科技有限公司	28	28
河南灵创电子科技有限公司	25	25
北京圣博润高新技术股份有限公司	20	20
杭州迪普科技股份有限公司	14	0
山东云天安全技术有限公司	7	7
上海观安信息技术股份有限公司	7	7
银行卡检测中心	4	4
新疆海狼科技有限公司	4	4
北京智游网安科技有限公司	1	1
广州万方计算机科技有限公司	1	1
CNCERT 重庆分中心	30	30
CNCERT 河北分中心	8	8
CNCERT 天津分中心	6	6
CNCERT 甘肃分中心	3	3
CNCERT 吉林分中心	3	3
CNCERT 湖南分中心	2	2
CNCERT 广西分中心	2	2
CNCERT 浙江分中心	2	2
CNCERT 福建分中心	2	2

CNCERT 内蒙古分中心	2	2
CNCERT 山西分中心	2	2
CNCERT 河南分中心	2	2
CNCERT 上海分中心	1	1
CNCERT 江西分中心	1	1
个人	416	416
报送总计	2946	2227

本周漏洞按类型和厂商统计

本周，CNVD 收录了 554 个漏洞。应用程序 293 个，WEB 应用 89 个，网络设备（交换机、路由器等网络端设备）52 个，智能设备（物联网终端设备）47 个，操作系统 45 个，安全产品 25 个，数据库 3 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序	293
WEB 应用	89
网络设备（交换机、路由器等网络端设备）	52
智能设备（物联网终端设备）漏洞	47
操作系统	45
安全产品	25
数据库	3

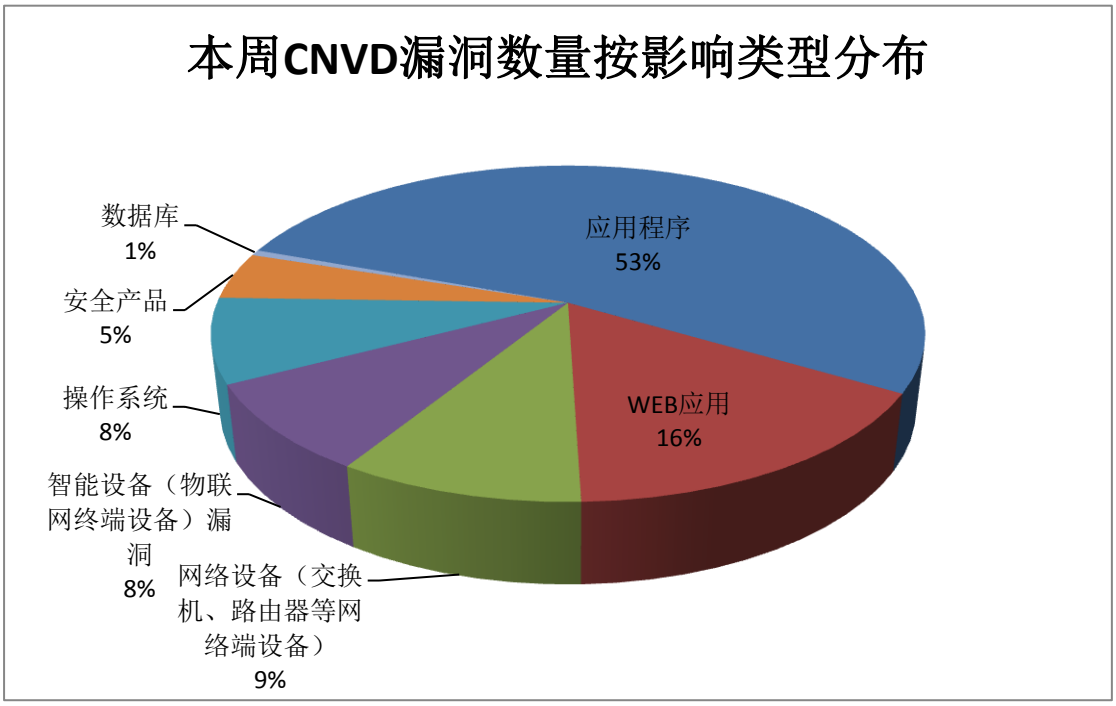

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、Cisco、Dell 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Apple	29	5%
2	Cisco	21	4%
3	Dell	20	4%
4	GitLab	20	4%
5	Intel	17	3%
6	Trend Micro	16	3%
7	Apache	13	2%
8	D-Link	12	2%
9	Magento	12	2%
10	其他	394	71%

本周行业漏洞收录情况

本周，CNVD 收录了 33 个电信行业漏洞，40 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“Moxa AWK-3131A 代码执行漏洞、Cisco MDS 9000 Series Multilayer Switches NX-OS Software 拒绝服务漏洞、Google Android FPC 组件权

限提升漏洞、Rockwell Automation Arena Simulation Software 代码执行漏洞、Synergy Systems & Solutions HUSKY RTU 6049-E70 输入验证错误漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

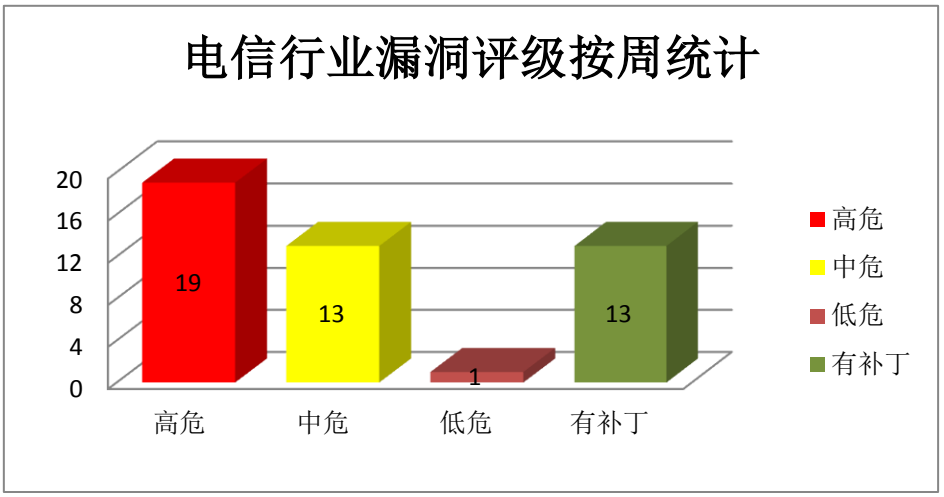

图 3 电信行业漏洞统计

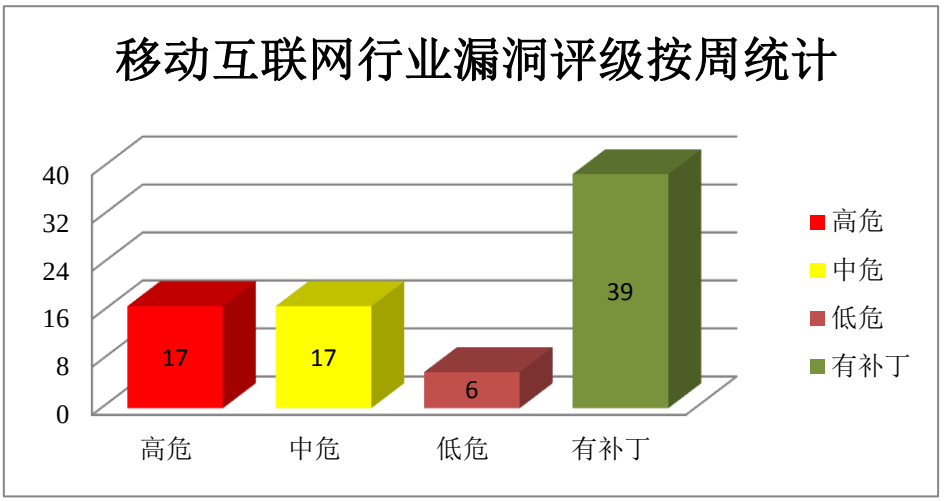

图 4 移动互联网行业漏洞统计

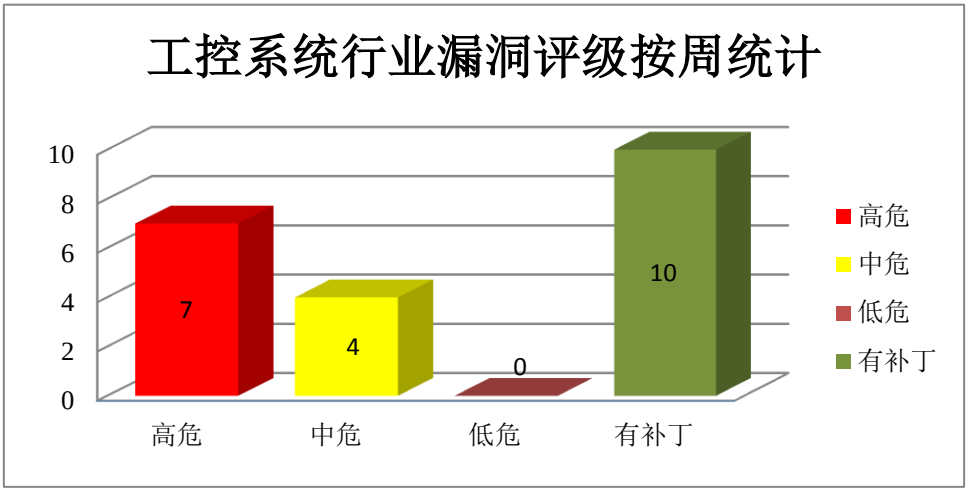

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Cisco 产品安全漏洞

Cisco FXOS Software 是美国思科（Cisco）公司的一套运行在思科安全设备中的防火墙软件。Cisco IP Conference Phone 7832 和 Cisco IP Conference Phone 8832 等都是 IP 电话系列产品。Supervisor 是一套适用于类 Unix 系统的过程控制系统。Cisco NX-OS Software 是一套交换机使用的数据中心级操作系统软件。Cisco MDS 9000 Series Multilayer Switches 是一款 MDS 9000 系列多层交换机。Cisco Prime Network Registrar（CPNR）是一款网络注册器产品。Cisco Intelligent Proximity 是一项创新功能集，可让您通过移动设备实现更丰富的协作体验。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco IP Phone 远程代码执行漏洞、Cisco FXOS Software 和 Cisco UCS Manager Software 操作系统命令注入漏洞、Cisco Nexus 1000V Switch for VMware vSphere 资源管理错误漏洞、Cisco FXOS Software 和 Cisco UCS Manager 操作系统命令注入漏洞、Cisco NX-OS Software 和 Cisco FXOS Software 输入验证错误漏洞（CNVD-2020-14813）、Cisco MDS 9000 Series Multilayer Switches NX-OS Software 拒绝服务漏洞、Cisco Prime Network Registrar 跨站请求伪造漏洞、Cisco Intelligent Proximity SSL 证书验证漏洞。其中，除“Cisco FXOS Software 和 Cisco UCS Manager Software 操作系统命令注入漏洞、Cisco FXOS Software 和 Cisco UCS Manager 操作系统命令注入漏洞”外，其余漏洞的综合评级为“高危”目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-14803

https://www.cnvd.org.cn/flaw/show/CNVD-2020-14810

https://www.cnvd.org.cn/flaw/show/CNVD-2020-14811

https://www.cnvd.org.cn/flaw/show/CNVD-2020-14812

https://www.cnvd.org.cn/flaw/show/CNVD-2020-14813

https://www.cnvd.org.cn/flaw/show/CNVD-2020-14814

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15700

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15703

2、Apple 产品安全漏洞

Apple iOS 是为移动设备所开发的一套操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。Apple tvOS 是一套智能电视操作系统。Apple watchOS 是一套智能手表操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，导致堆损坏。

CNVD 收录的相关漏洞包括：多款 Apple 产品 Kernel 组件内存破坏漏洞（CNVD-2020-15285、CNVD-2020-15286、CNVD-2020-15570）、多款 Apple 产品 Kernel 组件竞态条件漏洞、多款 Apple 产品 libxpc 组件越界读取漏洞（CNVD-2020-15293）、多款 Apple 产品 Kernel 组件类型混淆漏洞（CNVD-2020-15564）、多款 Apple 产品 libxpc 组件内存破坏漏洞（CNVD-2020-15565）、多款 Apple 产品内存破坏漏洞（CNVD-2020-15566）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-15285

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15286

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15287

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15293

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15564

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15565

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15566

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15570

3、GitLab 产品安全漏洞

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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，更改或删除其对该问题的评论等。

CNVD 收录的相关漏洞包括：GitLab 访问控制错误漏洞（CNVD-2020-15299、CNVD-2020-15494）、GitLab 信息泄露漏洞（CNVD-2020-15300、CNVD-2020-15485、CNVD-2020-15488、CNVD-2020-15490、CNVD-2020-15492）、GitLab 日志信息泄露漏洞。

目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-15299

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15300

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15485

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15488

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15490

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15492

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15493

https://www.cnvd.org.cn/flaw/show/CNVD-2020-15494

4、Dell 产品安全漏洞

DELL EMC Isilon 是美国戴尔（Dell）公司的一套适用于非结构化数据的横向扩展存储系统。OneFS 是运行在其中的一套操作系统。Dell EMC iDRAC9 是一套包含硬件和软件的系统管理解决方案。Dell EMC iDRAC7 是一套包含硬件和软件的系统管理解决方案。Dell EMC iDRAC8 是一套包含硬件和软件的系统管理解决方案。Dell KACE 部署设备可实现完全集成的系统配置解决方案。Dell EMC OpenManage Server Administrator（OMSA）是一套系统管理解决方案。Dell G3 3579 是一款笔记本电脑。Cheng Ming 3977 是一款台式计算机。Embedded Box PC 5000 是一款嵌入式箱式电脑。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：Dell EMC Isilon OneFS 授权问题漏洞、Dell EMC iDRAC7、iDRAC8 和 iDRAC9 授权问题漏洞 、Dell KACE Systems Management Appliance (K1000)代码执行漏洞、Dell EMC OpenManage Server Administrator web 参数篡改漏洞、Dell EMC OpenManage Server Administrator XML 外部实体（XXE）注入漏洞、多款 Dell 产品访问控制错误漏洞、Dell EMC iDRAC7、iDRAC8 和 iDRAC9 权限许可和访问控制漏洞、Dell EMC iDRAC7 和 iDRAC8 错误处理漏洞漏洞。其中，“Dell EMC Isilon OneFS 授权问题漏洞、Dell KACE Systems Management Appliance (K1000)代码执行漏洞、多款 Dell 产品访问控制错误漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2020-15714

http://www.cnvd.org.cn/flaw/show/CNVD-2020-15715

http://www.cnvd.org.cn/flaw/show/CNVD-2020-15722

http://www.cnvd.org.cn/flaw/show/CNVD-2020-15723

http://www.cnvd.org.cn/flaw/show/CNVD-2020-15724

http://www.cnvd.org.cn/flaw/show/CNVD-2020-15720

http://www.cnvd.org.cn/flaw/show/CNVD-2020-15727

http://www.cnvd.org.cn/flaw/show/CNVD-2020-15728

5、Red Hat CloudForms 命令执行漏洞

Red Hat CloudForms 是美国红帽（Red Hat）公司的一套混合基础架构管理平台。本周，Red Hat CloudForms 被披露存在命令执行漏洞。攻击者可利用该漏洞以 root 用户身份执行任意的 shell 命令。目前，厂商尚未发布上述漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-15945

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list.htm

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2020-15110	Trend Micro Antivirus for Mac UrlfWTPPagePtr KERedirect 权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://esupport.trendmicro.com/en-US/home/pages/technical-support/1121296.aspx
CNVD-2020-15129	WordPress Time Capsule plugin 授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，及时更新：https://nvd.nist.gov/vuln/detail/CVE-2020-8771
CNVD-2020-15510	FasterXML jackson-databind 远程代码执行漏洞（CNVD-2020-15510）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/FasterXML/jackson-databind/issues/2634
CNVD-2020-15515	Moxa AWK-3131A 代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.moxa.com/en/support/support/security-advisory/awk-3131a-series-industrial-ap-bridge-client-vulnerabilities
CNVD-2020-15520	Facebook HHVM 缓冲区溢出漏洞（ CNVD-2020-15520）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://hhvm.com/blog/2020/02/20/security-update.html
CNVD-2020-15937	CloudBees Jenkins Script Security Plugin 输入验证错误漏洞（CNVD-2020-15937）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://products.enorth.com.cn/bfnrglxt/index.shtml

CNVD-2020-15942	Google Android FPC 组件权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2020-03-01
CNVD-2020-15979	多款 IBM 产品权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/3357549
CNVD-2020-15980	D-Link DWL-2600AP 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10113
CNVD-2020-15987	Microsoft Windows 和 Windows Server 权限提升漏洞	高	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/zh-CN/security-guidance/advisory/CVE-2020-0818

小结：本周，Cisco 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，导致拒绝服务等。此外，Apple、GitLab、Dell 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，获取敏感信息，执行任意代码，导致堆损坏等。另外，Red Hat CloudForms 被披露存在命令执行漏洞。攻击者可利用该漏洞以 root 用户身份执行任意的 shell 命令。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、Tenda N301 拒绝服务漏洞

验证描述

Tenda N301 是一款 11N 无线宽带路由器。

Tenda N301 中的 goform/setSysTools 存在拒绝服务漏洞，攻击者可通过零 wanMTU 值利用该漏洞导致设备崩溃。

验证信息

POC 链接：https://github.com/Gr3gPr1est/BugReport/blob/master/CVE-2019-16412.pdf

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-15765

信息提供者

华为技术有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. CVE-2019-0090 漏洞影响过去 5 年中发布的英特尔芯片

Positive Technologies 的安全专家警告，被跟踪为 CVE-2019-0090 的漏洞影响了过去 5 年中发布的所有 Intel 处理器，且该漏洞目前无法修补，并可能被攻击者利用以绕过所有启用硬件的安全保护。

参考链接：https://securityaffairs.co/wordpress/99120/hacking/intel-cve-2019-0090-flaw.html

2. 黑客们正试图接管数万个 WordPress 网站

威胁参与者正在发起黑客活动，旨在通过利用关键漏洞来占领数以万计的 WordPress 网站。其中包括利用了 WooCommerce 插件的一个 0day 漏洞，而该插件有 20000 多个安装。

参考链接：https://securityaffairs.co/wordpress/98685/hacking/wordpress-sites-plugins-hacking.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537