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 16 日-2020 年 03 月 22 日　　2020 年第 12 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 365 个，其中高危漏洞 103 个、中危漏洞 172 个、低危漏洞 90 个。漏洞平均分值为 5.49。本周收录的漏洞中，涉及 0day 漏洞 112 个（占 30%），其中互联网上出现“CentOS Web Panel SQL 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 2662 个，与上周（2537 个）环比增加 5%。

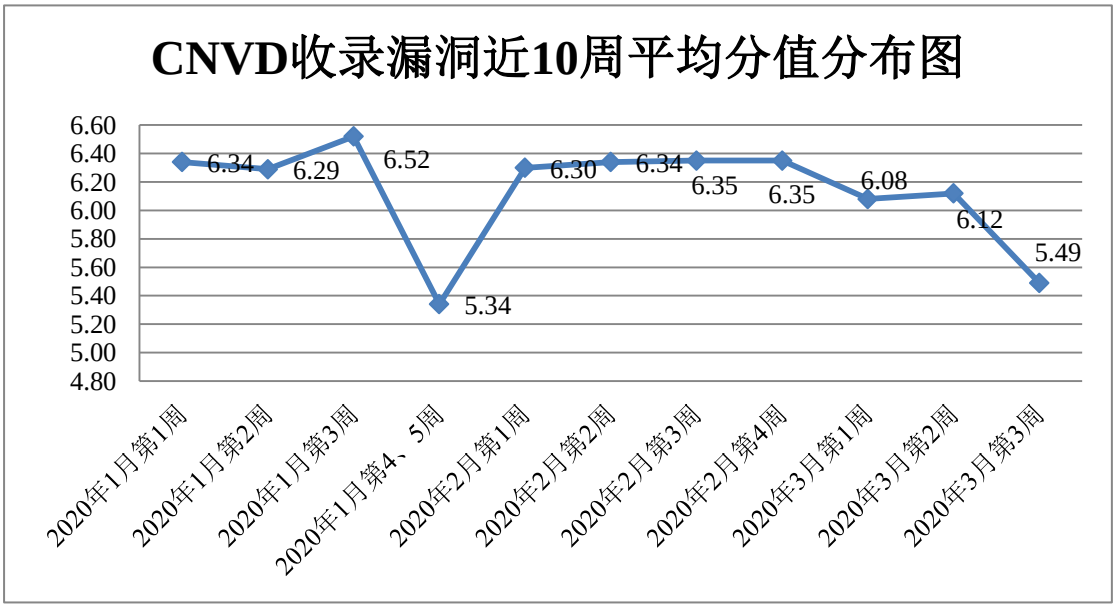

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 20 起，向基础电信企业通报漏洞事件 10 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 634 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 49 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7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：

国药控股宁夏有限公司、广州市三今网络技术有限公司、海南易而优科技有限公司、湖北淘码千维信息科技有限公司、上海商创网络科技有限公司、北京迪科远望科技有限公司、深圳市微控一指通科技有限公司、嘉兴想天信息科技有限公司、上海亿速网络科技有限公司、深圳市合信自动化技术有限公司、上海正航电子科技有限公司、上海茸易科技有限公司、苏州科达科技股份有限公司、上海秀可视科技有限公司、珠海金山软件股份有限公司、深圳市圆梦云科技有限公司、湖南第五元素网络科技开发有限公司、湖北国昇科技有限公司、镇江市云优网络科技有限公司、深圳市锟铻科技有限公司、北京超越极限信息技术有限公司、河南利梭互联网信息技术有限公司、北京海腾时代科技有限公司、南阳跃龙门科技有限公司、北京二六三企业通信有限公司、上海泛微网络科技股份有限公司、深圳极速创想科技有限公司、上海顶想信息科技有限公司、沈阳点动科技有限公司、青岛易软天创网络科技有限公司、山东思达特测控设备有限公司、深圳市迪元素科技有限公司、北京雄智伟业软件有限公司、南宁市传导网络技术有限责任公司、广州盈可视电子科技有限公司、北京良精志诚科技有限责任公司、郑州维维信息技术有限公司、北京通达信科科技有限公司、北京火绒网络科技有限公司、北京畅想之星信息技术有限公司、上海丹帆网络科技有限公司、海南赞赞网络科技有限公司、信呼、百易网络、zzz 中文网、YIXUNCMS 软件工作室、Accel-PPP、UQCMS、YCCMS、typecho、SeaCMS、Heybbs、Guojiz、The Apache Software Foundation 和 XYCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，恒安嘉新(北京)科技股份公司、北京天融信网络安全技术有限公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。南京众智维信息科技有限公司、北京铭图天成信息技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、山东新潮信息技术有限公司、河南灵创电子科技有限公司 、长春嘉诚信息技术股份有限公司、内蒙古奥创科技有限公司、北京机沃科技有限公司、杭州迪普科技股份有限公司、北京圣博润高新技术股份有限公司、国瑞数码零点实验室、北京华云安信息技术有限公司、杭州海康威视数字技术股份有限公司、深圳市魔方安全科技有限公司、河北千诚电子科技有限公司、辽宁北方实验室有限公司、南瑞集团公司（国网电力科学研究院）、北京冠程科技有限公司、山东云天安全技术有限公司、北京智游网安科技有限公司、天津市兴先道科技有限公司、星云博创科技有限公司及其他个人白帽子向 CNVD 提交了2662 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 2112 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）	979	979
奇安信网神（补天平台）	758	758
上海交大	375	375
恒安嘉新(北京)科技股份公司	303	0
北京天融信网络安全技术有限公司	300	5
哈尔滨安天科技集团股份有限公司	261	0
华为技术有限公司	155	0
深信服科技股份有限公司	150	0
新华三技术有限公司	72	0
北京神州绿盟科技有限公司	69	7
北京启明星辰信息安全技术有限公司	69	3
中新网络信息安全股份有限公司	41	41
北京数字观星科技有限公司	30	0
北京奇虎科技有限公司	25	0
中国电信集团系统集成有限责任公司	16	0
南京联成科技发展股份有限公司	13	13
北京安信天行科技有限公司	8	8
西安四叶草信息技术有限公司	7	7
沈阳东软系统集成工程有限公司	6	6
北京知道创宇信息技术股份有限公司	6	1

南京铱迅信息技术股份有限公司	1	1
杭州安恒信息技术股份有限公司	1	1
南京众智维信息科技有限公司	100	100
北京铭图天成信息技术有限公司	94	94
远江盛邦（北京）网络安全科技股份有限公司	68	68
山东新潮信息技术有限公司	39	39
河南灵创电子科技有限公司	34	34
长春嘉诚信息技术股份有限公司	28	28
内蒙古奥创科技有限公司	18	18
北京机沃科技有限公司	18	18
杭州迪普科技股份有限公司	15	0
北京圣博润高新技术股份有限公司	12	12
国瑞数码零点实验室	10	10
北京华云安信息技术有限公司	9	9
杭州海康威视数字技术股份有限公司	5	5
深圳市魔方安全科技有限公司	3	3
河北千诚电子科技有限公司	2	2
辽宁北方实验室有限公司	1	1
南瑞集团公司（国网电力科学研究院）	1	1
北京冠程科技有限公司	1	1
山东云天安全技术有限公司	1	1
北京智游网安科技有限公司	1	1

天津市兴先道科技有限公司	1	1
星云博创科技有限公司	1	1
CNCERT 西藏分中心	4	4
CNCERT 内蒙古分中心	2	2
CNCERT 甘肃分中心	2	2
CNCERT 吉林分中心	1	1
CNCERT 四川分中心	1	1
个人	345	345
报送总计	4117	2662

本周漏洞按类型和厂商统计

本周，CNVD 收录了 365 个漏洞。应用程序 224 个，WEB 应用 89 个，网络设备（交换机、路由器等网络端设备）26 个，操作系统 21 个，安全产品 3 个，智能设备（物联网终端设备）2 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	224
WEB 应用	89
网络设备（交换机、路由器等网络端设备）	26
操作系统	21
安全产品	3
智能设备（物联网终端设备）漏洞	2

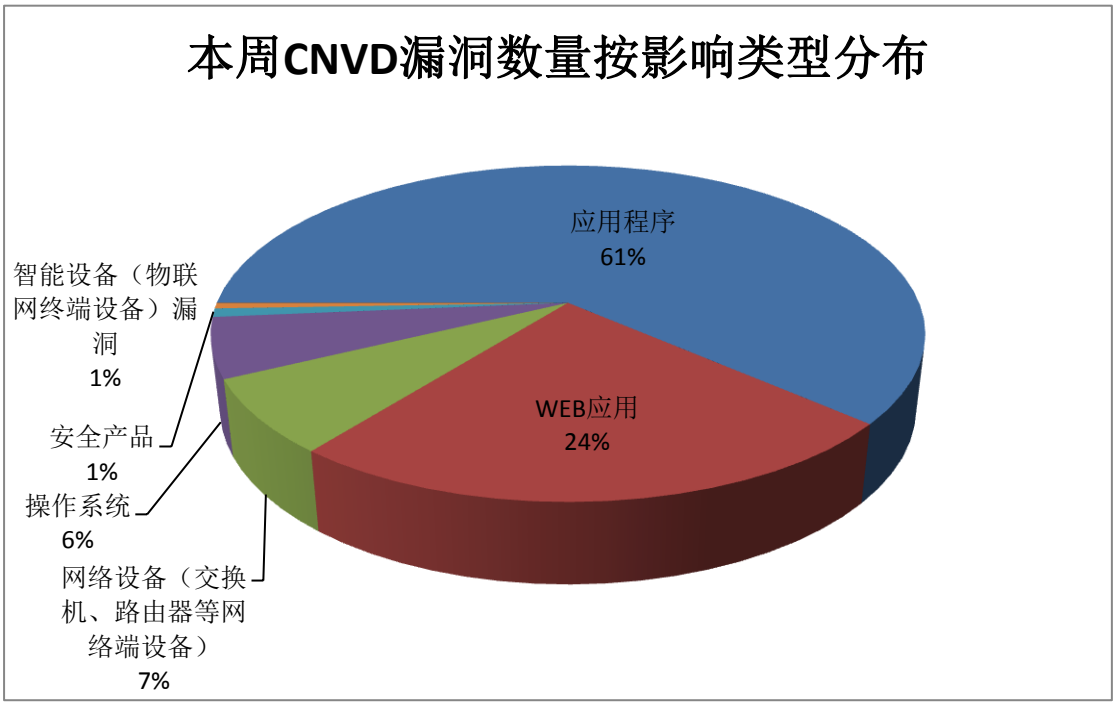

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Intel、Adobe、Microsoft 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	Intel	60	17%
2	Adobe	40	11%
3	Microsoft	16	4%
4	Google	12	3%
5	CloudBees	11	3%
6	cPanel	11	3%
7	GitLab	11	3%
8	WAGO	11	3%
9	IBM	10	3%
10	其他	183	50%

本周行业漏洞收录情况

本周，CNVD 收录了 13 个电信行业漏洞，13 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“多款 Moxa 产品缓冲区溢出漏洞、Google Android Netlink driver 越界写入漏洞、Delta Electronics CNCSoft ScreenEditor 缓冲区溢出漏洞（C

NVD-2020-17485）、Intel Converged Security and Management Engine、Server Platform Services 和 Trusted Execution Engine HECI subsystem 权限许可和访问控制问题漏洞”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/

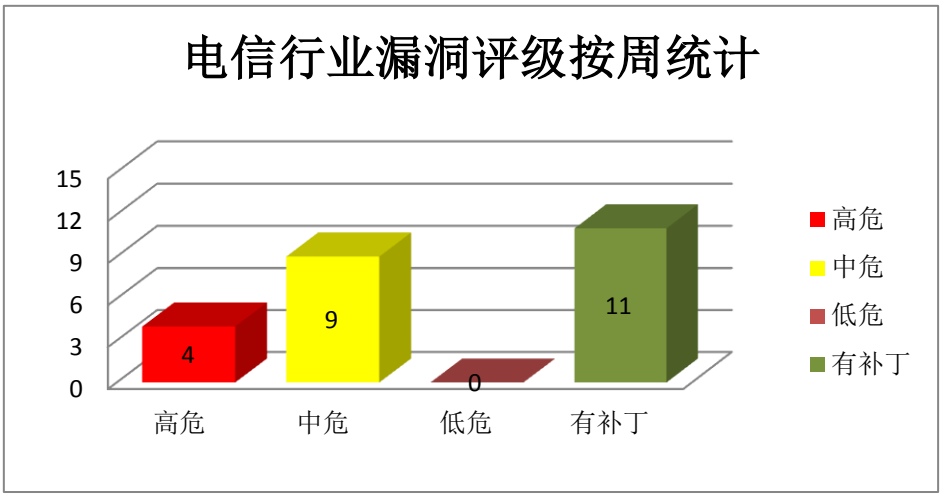

图 3 电信行业漏洞统计

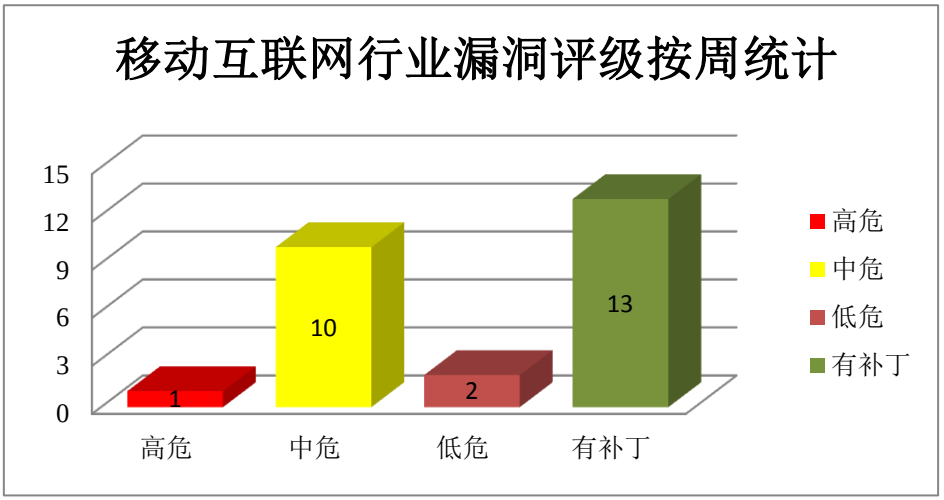

图 4 移动互联网行业漏洞统计

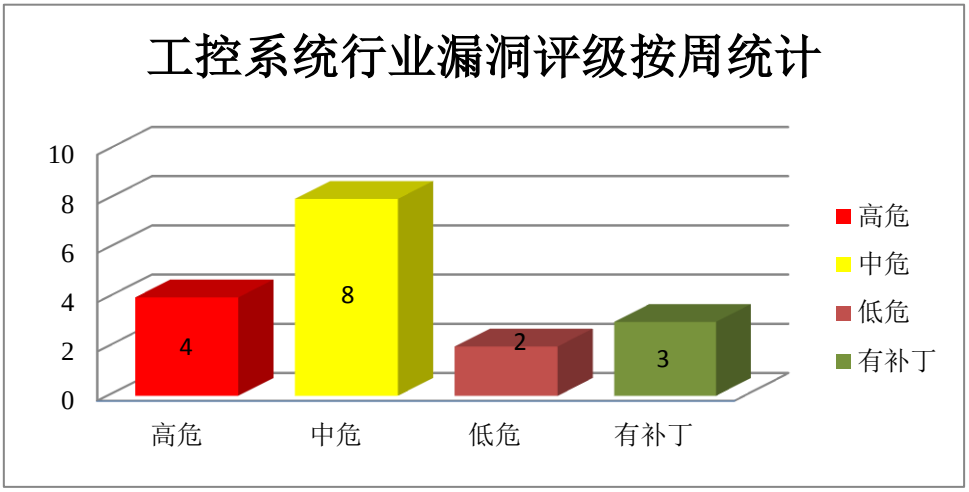

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。IIS Server 是其中的一个 IIS（互联网信息服务）服务器。Windows Graphics Device Interface（GDI）是其中的一个图形设备接口。Defender Security Center 是其中的一个计算机安全防护组件。Windows Installer 是其中的一个基于 Windows 系统中的工具组件，主要用于管理和配置软件服务。Microsoft Word 是一套 Office 套件中的文字处理软件。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，获取敏感信息等。

CNVD 收录的相关漏洞包括：Microsoft IIS 服务器篡改漏洞、Microsoft Windows GDI 信息泄漏漏洞（CNVD-2020-18166）、Microsoft Windows Defender Security Center 提权漏洞（CNVD-2020-18167、CNVD-2020-18165）、Microsoft Windows Installer 提权漏洞（CNVD-2020-18389、CNVD-2020-18388）、Microsoft Windows Graphics Device Interface 信息泄露漏洞（CNVD-2020-18394）、Microsoft Word 远程代码执行漏洞（CNVD-2020-18523）。其中 “Microsoft IIS 服务器篡改漏洞、Microsoft Windows Graphics Device Interface 信息泄露漏洞（CNVD-2020-18394）、Microsoft Word 远程代码执行漏洞（CNVD-2020-18523）”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-2020-18162

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18166

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18165

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18167

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18388

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18389

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18394

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18523

2、Intel 产品安全漏洞

8th Generation Intel Core Processor 和 7th Generation Intel Core Processor 都是美国英特尔（Intel）公司的产品。8th Generation Intel Core Processor 是一款第八代 Core 系列中央处理器（CPU）。7th Generation Intel Core Processor 是一款第七代 Core 系列中央处理器（CPU）。Intel 6th Generation Core Processors 是第六代 Core（酷睿）系列中央处理器（CPU）产品。Intel Converged Security and Management Engine 是一款安全管理引擎。Intel Server Platform Services 是一款服务器平台服务程序。Kernel subsystem 是其中的一个内核子系统。Intel TXE 是一款使用在 CPU（中央处理器）中具有硬件验证功能的信任执行引擎。Intel Core Processors 是一款 Intel Core 系列中央处理器（CPU）。Intel Xeon Processors 是一款 Intel Xeon 系列中央处理器（CPU）。Intel Trusted Execution Technology（TXT）是其中的一个可信执行技术组件。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，执行任意代码或导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：Intel 8th Generation Intel Core Processor 和 7th Generation Intel Core Processor 权限许可和访问控制问题漏洞（CNVD-2020-18568、CNVD-2020-18567）、Intel Converged Security and Management Engine 和 Intel Server Platform Services Kernel subsystem 授权问题漏洞、Intel TXE 和 Intel Converged Security and Management Engine 代码注入漏洞、Intel TXE 和 Intel Converged Security and Management Engine 权限许可和访问控制问题漏洞、Intel Converged Security and Management Engine 缓冲区溢出漏洞、Intel 6th Generation Core Processors 及后系列缓冲区溢出漏洞（CNVD-2020-18605）、Intel Core Processors 和 Intel Xeon Processors Intel TXT 缓冲区溢出漏洞。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-2020-18567

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18568

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18574

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18578

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18585

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18591

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18605

https://www.cnvd.org.cn/flaw/show/CNVD-2020-18606

3、Google 产品安全漏洞

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。Bluetooth 是其中的一个蓝牙组件。System 是其中的一个系统组件。Netlink driver 是其中的一个 Netlink 通信驱动程序。Framework 是其中的一个 Android 框架组件。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，提升权限。

CNVD 收录的相关漏洞包括：Google Android System 越界读取漏洞（CNVD-2020-17463、CNVD-2020-17464）、Google Android Netlink driver 越界写入漏洞、Google Android 缓冲区溢出漏洞（CNVD-2020-17484）、Google Android Framework 权限提升漏洞（CNVD-2020-17499、CNVD-2020-17501）、Google Android Bluetooth 缓冲区溢出漏洞（CNVD-2020-17377、CNVD-2020-17501）。其中“Google Android Netlink driver 越界写入漏洞”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-2020-17377
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17463
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17464
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17467
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17484
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17499
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17500
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17501

4、Adobe 产品安全漏洞

Adobe Photoshop，简称“PS”，是由 Adobe 公司开发和发行的图像处理软件。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。

CNVD 收录的相关漏洞包括：Adobe Photoshop 缓冲区溢出漏洞（CNVD-2020-17966、CNVD-2020-17975、CNVD-2020-17967、CNVD-2020-17976、CNVD-2020-17977、CNVD-2020-17978）、Adobe Photoshop 越界写入漏洞（CNVD-C-2020-51496、CNVD-2020-17973）。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-2020-17966
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17967
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17973
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17974
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17975
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17976

https://www.cnvd.org.cn/flaw/show/CNVD-2020-17977

https://www.cnvd.org.cn/flaw/show/CNVD-2020-17978

5、Adaware antivirus 权限提升漏洞

Lavasoft Adaware antivirus 是加拿大 Lavasoft 公司的一套杀毒软件。本周，Lavasoft Adaware antivirus 被披露存在权限提升漏洞。远程攻击者可借助恶意的 DLL 利用该漏洞提升权限。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-2020-18158

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-2020-17201	CloudBees Jenkins 资源管理错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jenkins.io/security/advisory/2012-01-12/
CNVD-2020-17379	VMware Workstation Virtual Printer 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://www.vmware.com/security/advisories/VMSA-2020-0004.html
CNVD-2020-17483	Dell EMC XtremIO XMS 跨站点脚本漏洞	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.dell.com/support/security/zh-cn/details/539703/DSA-2019-172-Dell-EMC-XtremIO-Security-Update-for-Multiple-Vulnerabilities
CNVD-2020-17614	IBM Sterling Connect:Direct 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：http://www.ibm.com/support/docview.wss?uid=ibm10875386
CNVD-2020-18087	Cisco Webex Network Recording Player 和 Webex Player 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-webex-player
CNVD-2020-18156	Foxit Studio Photo 缓冲区溢出漏洞（CNVD-2020-18156）	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.foxitsoftware.com/support/security-bulletins.php

CNVD-2020-18164	ZOHO ManageEngine OpManager 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.manageengine.com/network-monitoring/help/read-me-complete.html#125108
CNVD-2020-18169	WordPress RegistrationMagic SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wordpress.org/plugins/custom-registration-form-builder-with-submission-manager/#developers
CNVD-2020-18540	SAP Solution Manager 授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=540935305
CNVD-2020-18556	cPanel 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://documentation.cpanel.net/display/CL/84+Change+Log

小结：本周，Microsoft 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，获取敏感信息等。此外 Intel、Google、Adobe 等多款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，提升权限，执行任意代码，导致缓冲区溢出或堆溢出等。另外，Lavasoft Adaware antivirus 被披露存在权限提升漏洞。远程攻击者可借助恶意的 DLL 利用该漏洞提升权限。

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、CentOS Web Panel SQL 注入漏洞

验证描述

CentOS Web Panel (CWP)是一款免费的 Web 托管控制面板，可让您无需为需要完成的每项小任务而通过 SSH 访问服务器即可轻松管理多个服务器。

CentOS Web Panel 存在 SQL 注入漏洞。攻击者可通过/cwp_{SESSION_HASH}/admin/loader_ajax.php term 参数利用该漏洞进行 SQL 注入攻击。

验证信息

POC 链接：https://www.exploit-db.com/exploits/48212

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-17469

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. 思科在其 SD-WAN 产品中解决了多个漏洞

Cisco 已经解决了其 SD-WAN 解决方案中的五个漏洞，包括三个高严重性缺陷。攻击者可利用此漏洞对系统进行未经授权的更改，插入使用 root 权限执行的任意命令，并将权限提升到 root。

参考链接：https://securityaffairs.co/wordpress/99954/security/cisco-sd-wan-product-flaws.html

2. 大多数组织尚未修复 CVE-2020-0688 Microsoft Exchange 安全漏洞

组织在修补 Microsoft Exchange Server 漏洞（CVE-2020-0688）时有所延迟，该漏洞是 Microsoft 在 2020 年 2 月补丁日更新中修复的。该漏洞位于 Exchange 控制面板（ECP）组件，根本原因是 Exchange 服务器未能正确地创建在安装时的唯一密钥。

参考链接：https://securityaffairs.co/wordpress/99752/hacking/companies-cve-2020-0688-fixed.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