国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 11 月 09 日-2020 年 11 月 15 日　　2020 年第 46 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 716 个，其中高危漏洞 247 个、中危漏洞 390 个、低危漏洞 79 个。漏洞平均分值为 6.00。本周收录的漏洞中，涉及 0day 漏洞 471 个（占 66%），其中互联网上出现“QEMU OS 命令注入漏洞、Wordpress EZ-done File Manager 远程文件上传漏洞”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 4094 个，与上周（3727 个）环比增加 10%。

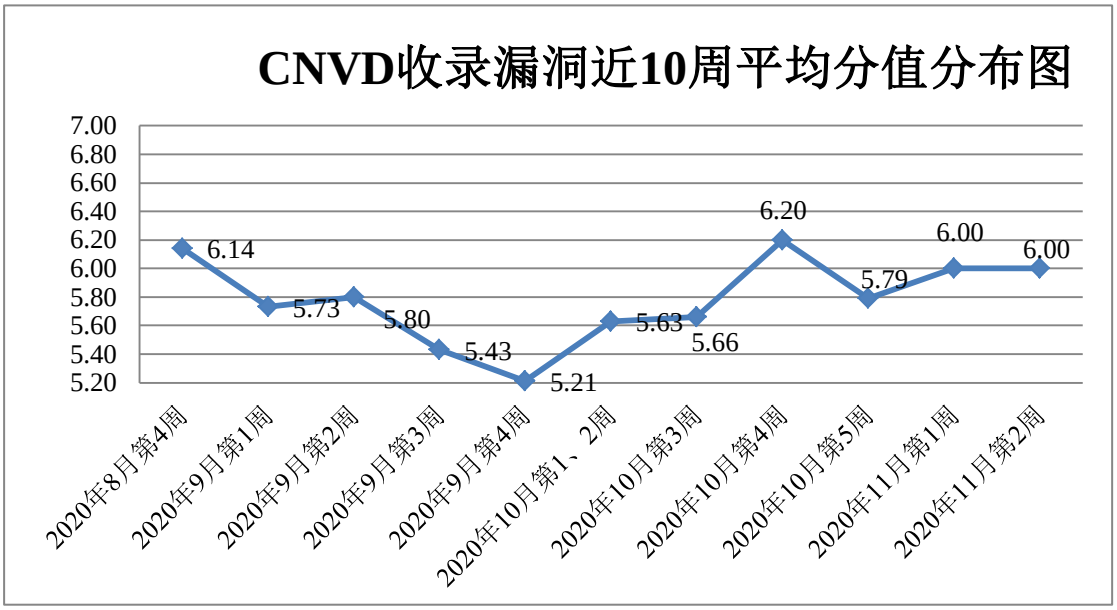

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 16 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 365 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 93 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 35 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：

上海雍熙信息技术有限公司、台湾百邇來網頁設計公司、铭飞科技有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、南宁迈世信息技术有限公司、河钢集团财智云科技有限公司、北京星网锐捷网络技术有限公司、北京辰信领创信息技术有限公司、武汉贝云网络科技有限公司、武汉京伦科技开发有限公司、深圳市乙辰科技股份有限公司、天津南大通用数据技术股份有限公司、厦门科华恒盛股份有限公司、呼和浩特市开企科技有限责任公司、浙江深大智能科技有限公司、重庆逐越光电科技有限公司、北京印象笔记科技有限公司、北京我知科技有限公司、北京安天网络安全技术有限公司、乐融致新电子科技（北京）有限公司、深圳市吉祥腾达科技有限公司、深圳市微客互动有限公司、云南天人网络科技有限公司、瑞芯微电子股份有限公司、广州网易计算机系统有限公司、钉钉科技有限公司、北京网易有道计算机系统有限公司、济南华企文化传媒有限公司、哈尔滨伟成科技有限公司、太原迅易科技有限公司、浙江大华技术股份有限公司、盘古网络集团有限公司、北京中科汇联科技股份有限公司、广州海昇计算机科技有限公司、北京众望网络科技有限公司、江西铭软科技有限公司、成都风禾网络科技有限公司、北京翰博尔信息技术股份有限公司、沧州市凡诺广告传媒有限公司、汕头市三互科技有限公司、北京米尔伟业科技有限公司、深圳市百为通达科技有限公司、楚雄州点击网络技术服务有限公司、米酷资源网、成都零起飞网络、上海荃路软件开发工作室、微同科技、信呼、里程密 PHP 博客系统、nacos 、BloofoxCMS、ZZCMS、Zzzcms、XHCMS、Gila CMS 、PHPEMS 、Victor CMS 、tuzicms、Hancom 和 HuCart。

本周，CNVD 发布了《Microsoft 发布 2020 年 11 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5836

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、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。国瑞数码零点实验室、北京华云安信息技术有限公司、山东云天安全技术有限公司、北京天地和兴科技有限公司、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 、山东华鲁科技发展股份有限公司、广州市蓝爵计算机科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、上海纽盾科技股份有限公司、安徽

长泰信息安全服务有限公司、吉林谛听信息技术有限公司、北京零零信安科技有限公司、河南信安世纪科技有限公司、新疆海狼科技有限公司、中移（杭州）信息技术有限公司、四川哨兵信息科技有限公司、京东云安全、内蒙古奥创科技有限公司、上海观安信息技术股份有限公司、北京机沃科技有限公司、国家互联网应急中心、北京字节跳动科技有限公司、北京智游网安科技有限公司、北京长亭科技有限公司、御安信息技术有限公司、杭州漠坦尼科技有限公司（雷石安全实验室）、广州市云聚数据服务有限公司、广州安亿信软件科技有限公司、北京安华金和科技有限公司、山石网科通信技术股份有限公司及其他个人白帽子向 CNVD 提交了 4094 个以事件型漏洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 2446 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）	1483	1483
上海交大	521	521
奇安信网神（补天平台）	442	442
北京神州绿盟科技有限公司	299	40
北京天融信网络安全技术有限公司	232	6
哈尔滨安天科技集团股份有限公司	211	0
华为技术有限公司	161	0
深信服科技股份有限公司	107	0
新华三技术有限公司	81	0
北京启明星辰信息安全技术有限公司	57	0
北京数字观星科技有限公司	50	0
北京奇虎科技有限公司	33	13
中新网络信息安全股份有限公司	27	27
中国电信集团系统集成有限责任公司	14	14

北京知道创宇信息技术股份有限公司	3	0
腾讯安全云鼎实验室	1	0
国瑞数码零点实验室	248	248
北京华云安信息技术有限公司	84	84
山东云天安全技术有限公司	84	84
北京天地和兴科技有限公司	53	53
南京众智维信息科技有限公司	30	30
河南灵创电子科技有限公司	25	25
山东华鲁科技发展股份有限公司	24	24
广州市蓝爵计算机科技有限公司	20	20
远江盛邦（北京）网络安全科技股份有限公司	20	20
北京云科安信科技有限公司（Seraph 安全实验室）	18	18
杭州迪普科技股份有限公司	15	0
上海纽盾科技股份有限公司	15	15
安徽长泰信息安全服务有限公司	8	8
吉林谛听信息技术有限公司	8	8
北京零零信安科技有限公司	8	8
河南信安世纪科技有限公司	8	8
新疆海狼科技有限公司	7	7
中移（杭州）信息技术有限公司	5	5
四川哨兵信息科技有限公司	4	4
京东云安全	4	4

内蒙古奥创科技有限公司	3	3
上海观安信息技术股份有限公司	3	3
国家互联网应急中心	3	3
北京机沃科技有限公司	2	2
北京字节跳动科技有限公司	2	2
西门子（中国）有限公司	1	0
北京智游网安科技有限公司	1	1
北京长亭科技有限公司	1	1
御安信息技术有限公司	1	1
杭州漠坦尼科技有限公司（雷石安全实验室）	1	1
广州市云聚数据服务有限公司	1	1
广州安亿信软件科技有限公司	1	1
北京安华金和科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
CNCERT 天津分中心	12	12
CNCERT 青海分中心	4	4
CNCERT 贵州分中心	2	2
CNCERT 四川分中心	2	2
个人	834	834
报送总计	5286	4094

本周漏洞按类型和厂商统计

本周，CNVD 收录了 716 个漏洞。应用程序 351 个，WEB 应用 252 个，操作系统 41 个，网络设备（交换机、路由器等网络端设备）37 个，智能设备（物联网终端设备）

19 个，安全产品 10 个，数据库 6 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	351
WEB 应用	252
操作系统	41
网络设备（交换机、路由器等网络端设备）	37
智能设备（物联网终端设备）	19
安全产品	10
数据库	6

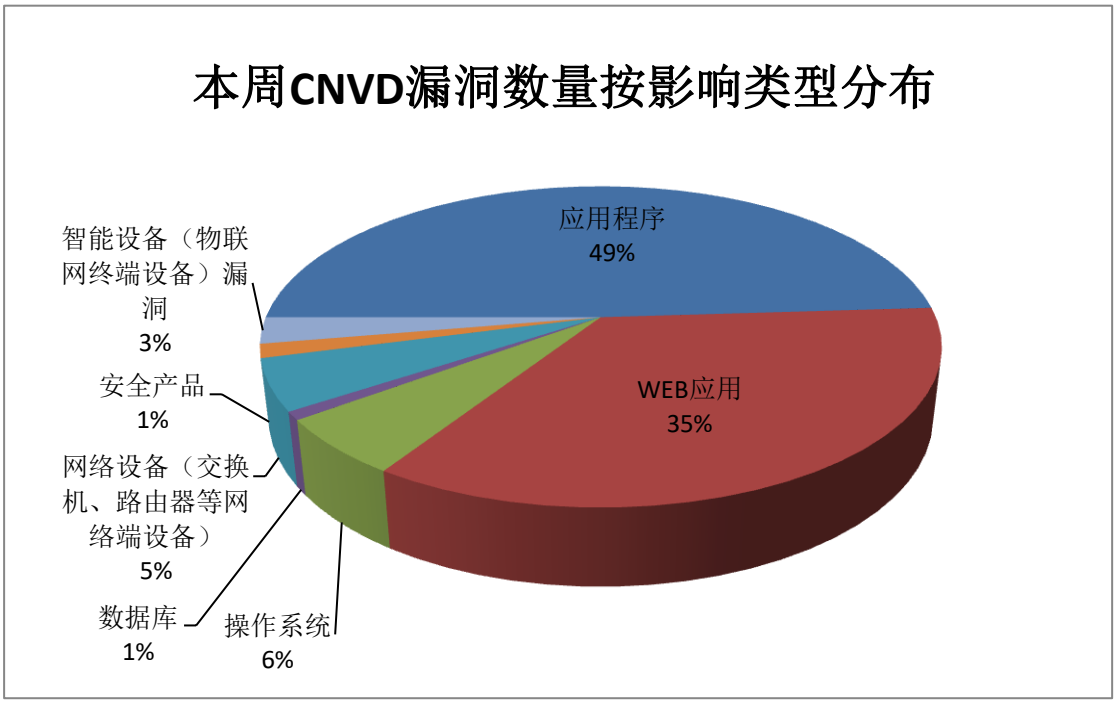

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、Hancom 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	Google	31	4%
2	Microsoft	30	4%
3	Hancom	20	3%
4	SAP	17	2%
5	CloudBees	17	2%
6	Apple	28	4%

7	上海展盟网络科技有限公司	14	2%
8	Observium	13	2%
9	Cisco	12	2%
10	其他	534	75%

本周行业漏洞收录情况

本周，CNVD 收录了 27 个电信行业漏洞，60 个移动互联网行业漏洞，46 个工控行业漏洞（如下图所示）。其中，“多款 Apple 产品资源管理错误漏洞 Google Android 缓冲区溢出漏洞（CNVD-2020-63213）、Cisco IOS XR -bit Preboot eXecution Environment 访问控制错误漏洞”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/

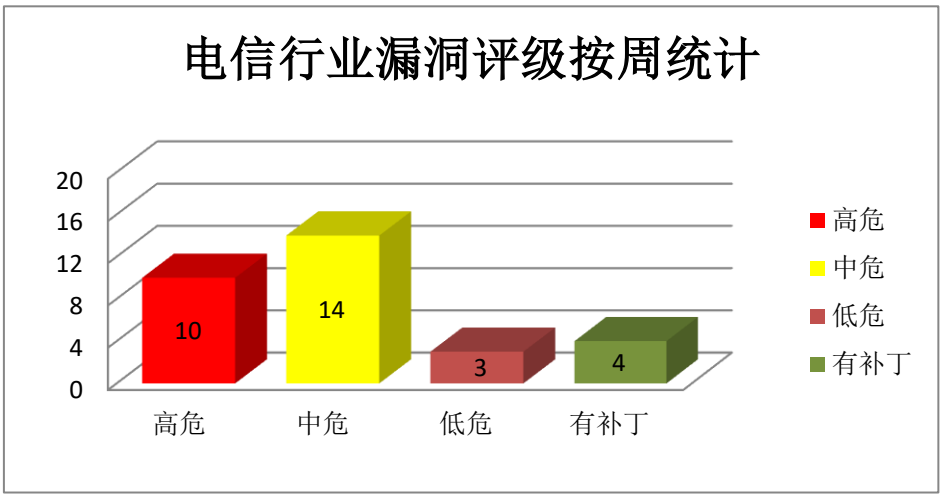

图 3 电信行业漏洞统计

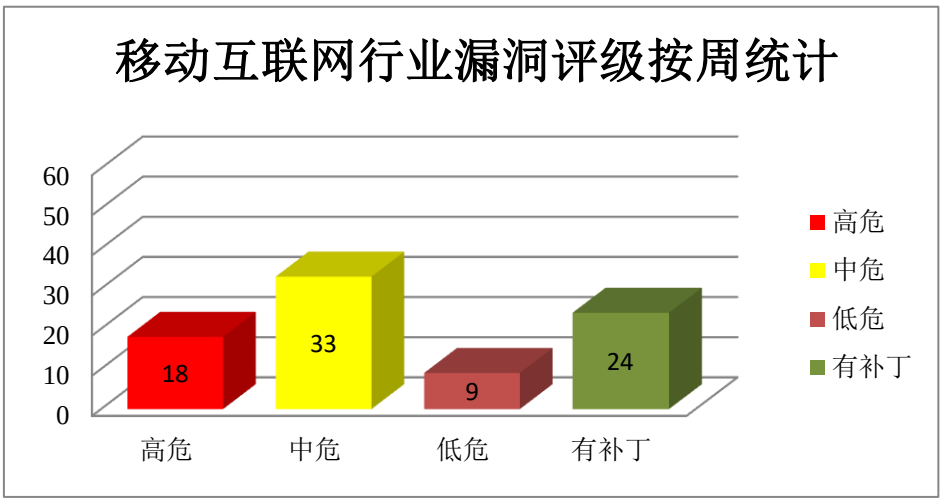

图 4 移动互联网行业漏洞统计

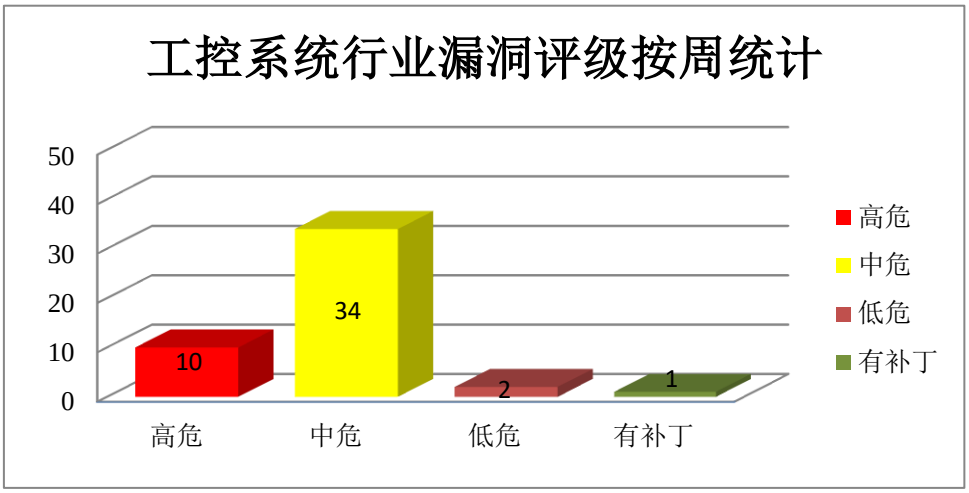

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。Microsoft Excel 是一款 Office 套件中的电子表格处理软件。Microsoft .NET Framework 是一种全面且一致的编程模型，也是一个用于构建 Windows、Windows Store、Windows Phone、Windows Server 和 Microsoft Azure 的应用程序的开发平台。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Edge PDF Reader 远程代码执行漏洞（CNVD-2020-61586、CNVD-2020-61593）、Microsoft Edge 远程代码执行漏洞（CNVD-2020-61587）、Microsoft Internet Explorer VBScript 远程代码执行漏洞（CNVD-2020-61605）、Microsoft Excel 远程代码执行漏洞（CNVD-2020-62335、CNVD-2020-62338）、Microsoft .NET Framework 远程代码执行漏洞（CNVD-2020-62333、CNVD-2020-62340）。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-2020-61586

https://www.cnvd.org.cn/flaw/show/CNVD-2020-61587

https://www.cnvd.org.cn/flaw/show/CNVD-2020-61593

https://www.cnvd.org.cn/flaw/show/CNVD-2020-61605

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62335

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62333

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62340

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62338

2、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。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，进行堆破坏等。

CNVD 收录的相关漏洞包括：Google Chrome 信息泄漏漏洞（CNVD-2020-61091）、Google Chrome 安全绕过漏洞（CNVD-2020-61101）、Google Chrome 资源管理错误漏洞（CNVD-2020-62477、CNVD-2020-62476、CNVD-2020-62475、CNVD-2020-62480、CNVD-2020-62479）、Google Chrome 缓冲区溢出漏洞（CNVD-2020-62478）。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-2020-61091

https://www.cnvd.org.cn/flaw/show/CNVD-2020-61101

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62477

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62476

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62475

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62480

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62479

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62478

3、Cisco 产品安全漏洞

Cisco IOS XR 是美国思科（Cisco）公司的一套为其网络设备开发的操作系统。Cisco SD-WAN vEdge 是是一款路由器。Cisco IP Phone 8800 Series 是一款 8800 系列的 IP 电话。Cisco Identity Services Engine (ISE)是下一代身份和访问控制策略平台，使企业能够执行合规性、增强基础架构安全性并简化其服务操作。Cisco SD-WAN Solution 是 Cisco 的一套网络扩展解决方案，vManage 是其中的控制台。Cisco Video Surveillance 8000 Series IP Cameras 是一款视频监控摄像头。Cisco FXOS Software 是一套运行在思科安全设备中的防火墙软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过限制，提升特权，进行跨站点请求伪造(CSRF)攻击，执行命令等。

CNVD 收录的相关漏洞包括：Cisco IOS XR -bit Preboot eXecution Environment 访问控制错误漏洞、Cisco SD-WAN vEdge 访问控制错误漏洞、Cisco IP Phone TCP 报文拒绝服务漏洞、Cisco Identity Services Engine 权限提升漏洞、Cisco SD-WAN vManage 命令注入漏洞（CNVD-2020-61949）、Cisco Video Surveillance 8000 Series IP Cameras 资源管理错误漏洞、Cisco FXOS 命令执行漏洞、Cisco FXOS 跨站请求伪造漏洞。其中，“Cisco IOS XR -bit Preboot eXecution Environment 访问控制错误漏洞、Cisco IP Phone TCP 报文拒绝服务漏洞、Cisco FXOS 命令执行漏洞”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-2020-61947

https://www.cnvd.org.cn/flaw/show/CNVD-2020-61946

https://www.cnvd.org.cn/flaw/show/CNVD-2020-61945

https://www.cnvd.org.cn/flaw/show/CNVD-2020-61951

https://www.cnvd.org.cn/flaw/show/CNVD-2020-61949

https://www.cnvd.org.cn/flaw/show/CNVD-2020-61954

https://www.cnvd.org.cn/flaw/show/CNVD-2020-61953

https://www.cnvd.org.cn/flaw/show/CNVD-2020-63200

4、SAP 产品安全漏洞

SAP Process Integration 是 SAP 的企业应用程序集成（EAI）软件，用于在公司中的 SAP 与非 SAP 应用程序之间或与公司外部的系统之间进行无缝集成。SAP Commerce Cloud 是面向 B2B、B2C 和 B2B2C 公司的云原生全渠道商务解决方案。SAP Netweaver 是一套面向服务的集成化应用平台。SAP Solution Manager 是一套集系统监控、SAP 支持桌面、自助服务、ASAP 实施等多个功能为一体的系统管理平台。SAP Business Objects Business Intelligence Platform 是一套商业智能软件和企业绩效解决方案套件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获取敏感信息，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：SAP Process Integration 信息泄露漏洞、SAP Commerce Cloud 信息泄露漏洞、SAP Commerce Cloud 服务器端请求伪造漏洞、SAP Commerce Cloud 拒绝服务漏洞、SAP NetWeaver 输入验证错误漏洞、SAP Solution Manager 未授权访问漏洞、SAP Solution Manager 内存破坏漏洞、SAP Business Objects Business Intelligence Platform 访问控制错误漏洞（CNVD-2020-62944）。其中，“SAP Commerce Cloud 拒绝服务漏洞”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-2020-62456

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62470

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62472

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62471

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62941

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62946

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62945

https://www.cnvd.org.cn/flaw/show/CNVD-2020-62944

5、QNAP Systems TS-870 跨站脚本漏洞（CNVD-2020-62488）

QNAP Systems TS-870 是一款 NAS（网络附属存储）设备。本周，QNAP Systems TS-870 被披露存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。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-2020-62488

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-2020-61925	CloudBees Jenkins Active Directory Plugin 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://www.jenkins.io/security/advisory/2020-11-04/#SECURITY-2117
CNVD-2020-61952	Cisco FXOS OS 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-cmdinj-pqZvmXCr
CNVD-2020-61981	QEMU 缓冲区溢出漏洞（CNVD-2020-61981）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://git.qemu.org/?p=qemu.git;a=commitdiff;h=da885fe1ee8b4589047484bd7fa05a4905b52b17
CNVD-2020-62251	Aruba Networks Aruba Airwave 远程命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04051en_us
CNVD-2020-62460	Foxit Reader 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.foxitsoftware.com/support/security-bulletins.html
CNVD-2020-63188	Palo Alto Networks Panorama 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security.paloaltonetworks.com/CVE-2020-2022
CNVD-2020-63210	Oracle Marketing--Marketing Administration 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://www.oracle.com/security-alerts/cpuoct2020.html
CNVD-2020-	Juniper Networks Junos OS	高	目前厂商已发布升级补丁以修复漏

63216	J-Web 跨站脚本漏洞		洞，补丁获取链接：https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11070
CNVD-2020-63215	Junos OS IPv6 数据报文拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11083
CNVD-2020-63213	Google Android 缓冲区溢出漏洞（CNVD-2020-63213）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/2020-10-01

小结：本周，Microsoft 产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。此外，Google、Cisco、SAP 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，，提升特权，获取敏感信息，进行跨站点请求伪造(CSRF)攻击，执行命令等。另外，QNAP Systems TS-870 被披露存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

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、QEMU OS 命令注入漏洞

验证描述

QEMU 是一套由法布里斯·贝拉(Fabrice Bellard)所编写的、以 GPL 许可证分发源码的模拟处理器，在 GNU/Linux 平台上使用广泛。

QEMU 4.0.0 及更早版本中的 QMP guest_exec 命令存在 OS 命令注入漏洞。攻击者可通过向侦听服务器发送特制 QMP 命令利用该漏洞实现代码执行或导致拒绝服务或信息泄露。

验证信息

POC 链接：https://fakhrizulkifli.github.io/posts/2019/06/06/CVE-2019-12929/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-61979

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. 酒店预订平台泄露 Booking.com 等在线预订网站的用户数据

西班牙巴塞罗那一家名为 Prestige Software 的软件公司被发现暴露了全球数百万客户的敏感、隐私和财务数据。尤其是来自 Booking.com、Expedia、Agoda、Amadeus、Hotels.com、Hotelbeds、Omnibees、Sabre 等几家公司的客户都是此次数据泄露事件的意外受害者。

参考链接：https://www.cnbeta.com/articles/tech/1050841.htm

2. Western Digital 发现 RPMB 漏洞影响多个供应商

Western Digital 的研究人员最近在重放保护存储块（RPMB）协议中发现了一个漏洞，该漏洞影响了其他几家主要公司的产品，包括 Google，Intel 和 MediaTek。

参考链接：https://www.securityweek.com/western-digital-finds-replay-attack-protection-flaw-affecting-multiple-vendors

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