

信息安全漏洞周报

2020年05月25日-2020年05月31日

2020年第22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 312 个，其中高危漏洞 92 个、中危漏洞 182 个、低危漏洞 38 个。漏洞平均分为 5.84。本周收录的漏洞中，涉及 0day 漏洞 121 个（占 39%），其中互联网上出现“WordPress Ultimate Member 跨站点请求伪造漏洞、OpenEMR 远程代码执行漏洞（CNVD-2018-14867）”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 3956 个，与上周（5021 个）环比减少 21%。

CNVD收录漏洞近10周平均分分布图

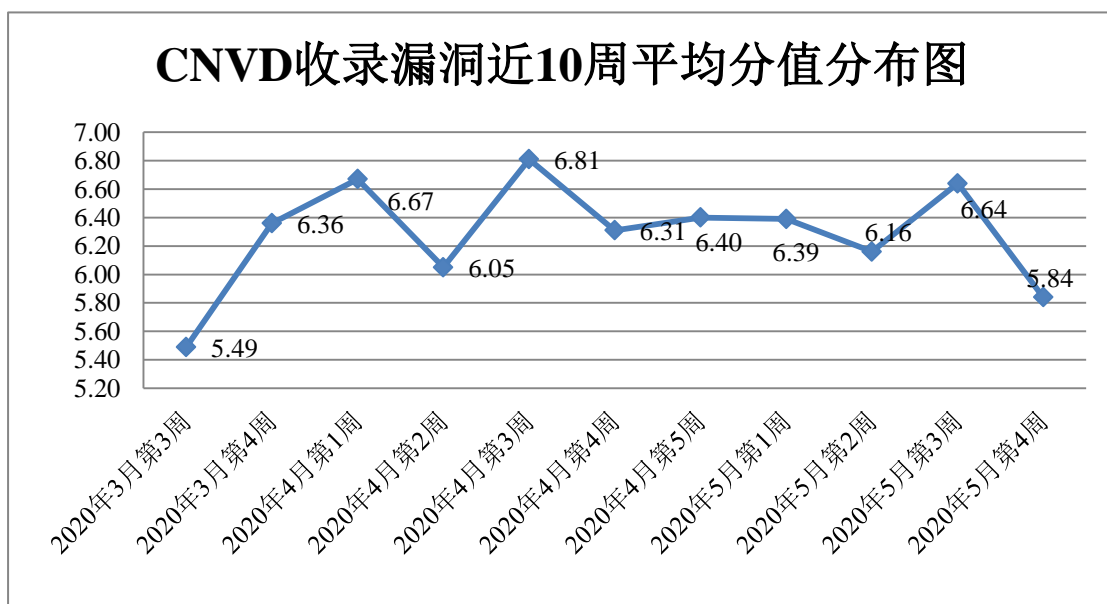


图 1 CNVD 收录漏洞近 10 周平均分分布图

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 22 起，向基础电信企业通报漏洞事件 12 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 252 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 27 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 24 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：

重庆逐越光电科技有限公司、杭州维克会网络科技有限公司、上海讯有信息科技有限公司、保定市互动企业营销策划有限公司、北京良精志诚科技有限责任公司、北京链家房地产经纪有限公司、大连公众信息产业集团有限公司、中建三局智能技术有限公司、深圳市国人在线信息技术有限公司、天择文化传播（河南）有限公司、微软(中国)有限公司、安徽省科迅教育装备有限公司、珠海金山办公软件有限公司石家庄市征红网络科技有限公司、雄帝股份有限公司、用友网络科技股份有限公司、廊坊市极致网络科技有限公司、淄博欧凯信息技术有限公司、茉柏桢（上海）软件科技有限公司、上海基分文化传播有限公司、洛阳云业信息科技有限公司、苏州烟火网络科技有限公司、上海海典软件股份有限公司、宜兴易发网络服务有限公司、西安佰联网络技术有限公司、中山市凝聚网络科技有限公司、东莞市鼎点网络科技有限公司、浙江大华技术股份有限公司、深圳市微客互动有限公司、福州极限软件开发有限公司、深圳市腾狐物联科技有限公司、上海顶想信息科技有限公司、北京智量科技有限公司、海南创想未来文化传媒有限公司、深圳市锟铻科技有限公司、海南赞赞网络科技有限公司、广州购啊购科技有限公司、广州齐博网络科技有限公司、湖南天牛网络科技有限公司、北京小米科技有限责任公司、南京医健通信息科技有限公司、锤子科技（北京）股份有限公司、成都依能科技股份有限公司、西门子（中国）有限公司、南京致汇达网络科技有限公司、青岛汇商传媒有限公司、厦门市好景科技有限公司、济南白菜网络技术有限公司、上海天健源达信息科技有限公司、湖北淘码千维信息科技有限公司、洪湖尔创网联信息技术有限公司、镇江市云优网络科技有限公司、北京地铁运营有限公司、台达电子企业管理（上海）有限公司、深圳市硕赢互动信息技术有限公司、武汉金百瑞科技股份有限公司、北京泛在时代教育技术有限责任公司、浙江省测绘大队、北京消防协会会、菏泽市定陶区子鸥网络科技服务中心、延边州石头网络科技服务中心、新秀工作室、点拓开发网、李雷博客、耳朵软件、万通 CMS、熊海 CMS、DM 建站系统、逍遥 B2C 商城系统、贴心猫(imcat)、Apache 软件基金会、大米 CMS、Guojiz、ZrLog、Cszcms、phpgurukul、Canonical、Emerson、PIMS、Rockwell 和 TuziCMS。

本周，CNVD 发布了《关于 ISC BIND 存在拒绝服务漏洞的安全公告》。详情参见 CNVD 网站公告内容。

<https://www.cnvd.org.cn/webinfo/show/5543>



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、中新网络信息安全股份有限公司、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、河南灵创电子科技有限公司、杭州迪普科技股份有限公司、北京墨云科技有限公司、山东云天安全技术有限公司、河北华测信息技术有限公司、广州安亿信软件科技有限公司、北京天地和兴科技有限公司、京东云安全、上海观安信息技术股份有限公司、北京长亭科技有限公司、北京浩瀚深度信息技术股份有限公司、杭州海康威视数字技术股份有限公司、北京华云安信息技术有限公司、星云博创科技有限公司、成都安美勤信息技术股份有限公司、北京智游网安科技有限公司、河南信安世纪科技有限公司、天津市兴先道科技有限公司、济南三泽信息安全测评有限公司及其他个人白帽子向 CNVD 提交了 2938 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 2147 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）	933	933
奇安信网神（补天平台）	690	690
上海交大	524	524
哈尔滨安天科技集团股份有限公司	276	0
中新网络信息安全股份有限公司	163	163
北京天融信网络安全技术有限公司	144	4
华为技术有限公司	137	0
恒安嘉新(北京)科技股份公司	131	0
新华三技术有限公司	89	0
北京神州绿盟科技有限公司	72	6
深信服科技股份有限公司	68	0
北京启明星辰信息安全技术有限公司	57	0

中国电信集团系统集成有 限责任公司	43	34
北京奇虎科技有限公司	34	34
北京数字观星科技有限公 司	30	0
杭州安恒信息技术股份有 限公司	10	10
北京知道创宇信息技术股 份有限公司	1	0
南京铱迅信息技术股份有 限公司	1	1
远江盛邦（北京）网络安 全科技股份有限公司	90	90
国瑞数码零点实验室	44	44
河南灵创电子科技有限公司	25	25
杭州迪普科技股份有限公 司	14	0
北京墨云科技有限公司	12	12
山东云天安全技术有限公 司	9	9
河北华测信息技术有限公 司	7	7
广州安亿信软件科技有限 公司	7	7
北京天地和兴科技有限公 司	5	5
京东云安全	5	5
上海观安信息技术股份有 限公司	2	2
北京长亭科技有限公司	2	2
北京浩瀚深度信息技术股 份有限公司	2	2
杭州海康威视数字技术股 份有限公司	1	1
北京华云安信息技术有限 公司	1	1
星云博创科技有限公司	1	1

成都安美勤信息技术股份有限公司	1	1
北京智游网安科技有限公司	1	1
河南信安世纪科技有限公司	1	1
天津市兴先道科技有限公司	1	1
济南三泽信息安全测评有限公司	1	1
CNCERT 天津分中心	9	9
CNCERT 湖南分中心	7	7
CNCERT 西藏分中心	7	7
CNCERT 广西分中心	6	6
CNCERT 贵州分中心	4	4
CNCERT 海南分中心	2	2
CNCERT 安徽分中心	2	2
CNCERT 上海分中心	2	2
CNCERT 河北分中心	1	1
个人	281	281
报送总计	3956	2938

本周漏洞按类型和厂商统计

本周，CNVD 收录了 312 个漏洞。应用程序 104 个，操作系统 94 个，WEB 应用 79 个，网络设备（交换机、路由器等网络端设备）27 个，数据库 6 个，安全产品 1 个，智能设备（物联网终端设备）1 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	104
操作系统	94
WEB 应用	79
网络设备（交换机、路由器等网络端设备）	27

数据库	6
安全产品	1
智能设备（物联网终端设备）漏洞	1

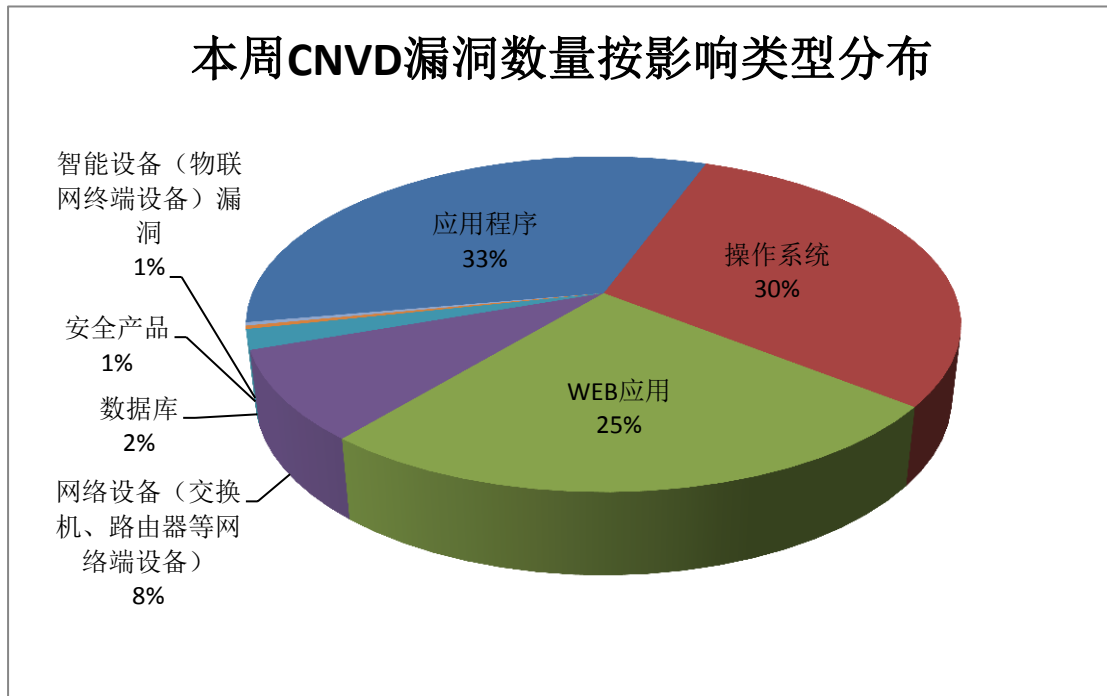


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、NETGEAR、珠海金山办公软件有限公司等多家厂商的产品，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	74	24%
2	NETGEAR	20	6%
3	珠海金山办公软件有限公司	20	6%
4	Advantech	11	4%
5	WordPress	11	4%
6	Apple	10	3%
7	Microsoft	10	3%
8	Oracle	10	3%
9	SAP	9	3%
10	其他	137	44%

本周，CNVD 收录了 26 个电信行业漏洞，87 个移动互联网行业漏洞，15 个工控行业漏洞（如下图所示）。其中，“多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2020-30762）、Samsung 移动设备缓冲区溢出漏洞（CNVD-2020-30408）、Advantech WebAccess Node 路径遍历漏洞（CNVD-2020-29743）”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/>

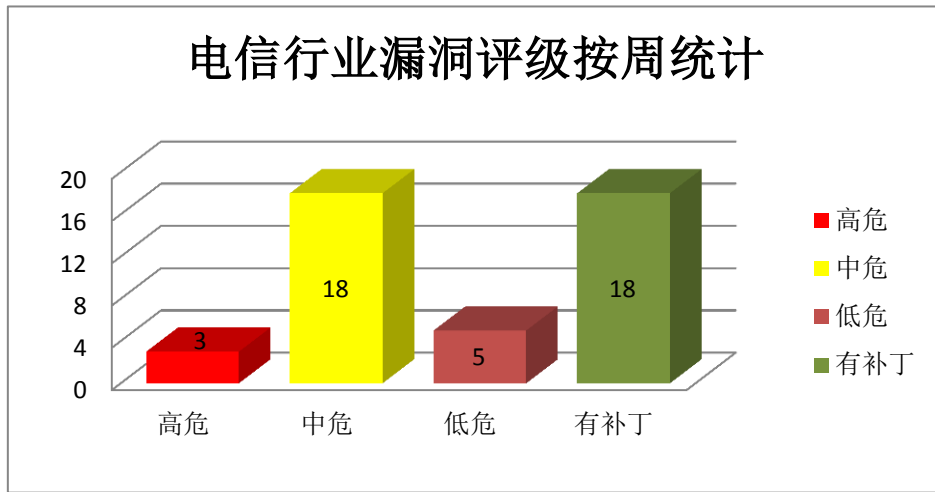


图 3 电信行业漏洞统计

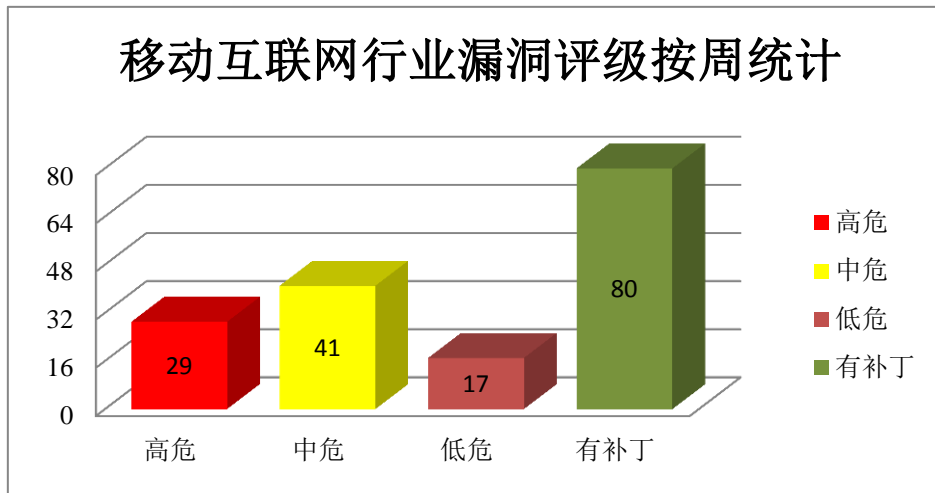


图 4 移动互联网行业漏洞统计

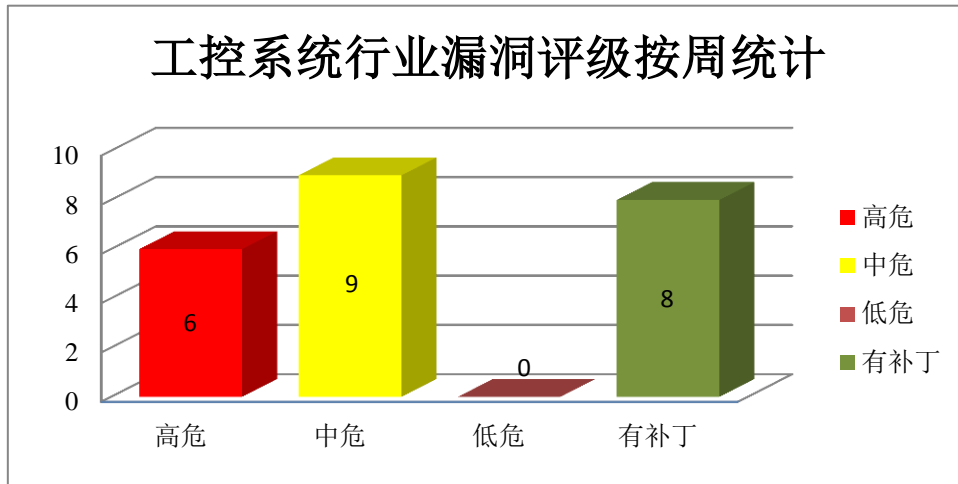


图 5 工控系统行业漏洞统计

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、Advantech 产品安全漏洞

Advantech WebAccess 是一个基于浏览器的 SCADA 软件包，用于监控、数据采集和可视化。它用于在需要远程操作的情况下自动化复杂的工业流程。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞覆盖应用程序控制范围之外的文件，获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：Advantech WebAccess Node 缓冲区溢出漏洞（CNVD-2020-29739、CNVD-2020-29740）、Advantech WebAccess Node 越界读取漏洞、Advantech WebAccess Node 路径遍历漏洞（CNVD-2020-29743、CNVD-2020-29744、CNVD-2020-29742）、Advantech WebAccess Node SQL 注入漏洞、Advantech WebAccess Node 输入验证错误漏洞。其中，“Advantech WebAccess Node 缓冲区溢出漏洞（CNVD-2020-29739、CNVD-2020-29740）、Advantech WebAccess Node 路径遍历漏洞（CNVD-2020-29743）、Advantech WebAccess Node 输入验证错误漏洞”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-2020-29740>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29739>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29738>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29743>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29742>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29741>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-27432>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29744>

2、Oracle 产品安全漏洞

Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。Oracle E-Business Suite 是在原来 Application(ERP) 基础上的扩展，包括 ERP（企业资源计划管理）、HR（人力资源管理）、CRM（客户关系管理）等等多种管理软件的集合，是无缝集成的一个管理套件。Oracle Advanced Outbound Telephony 是 Oracle Interaction Center 的模块，用于解决出站电话问题。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未经授权读取、更新、插入或删除数据。

CNVD 收录的相关漏洞包括：Oracle Weblogic Server 远程代码执行漏洞（CNVD-2020-29746、CNVD-2020-29745）、Oracle Advanced Outbound Telephony 未授权访问漏洞（CNVD-2020-29762、CNVD-2020-29767、CNVD-2020-29765、CNVD-2020-29764、CNVD-2020-29763、CNVD-2020-29766）。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-2020-29746>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29745>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29762>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29765>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29764>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29763>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29767>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29766>

3、SAP 产品安全漏洞

SAP Business Objects Business Intelligence Platform 是德国思爱普（SAP）公司的一套商业智能软件和企业绩效解决方案套件。SAP Adaptive Server Enterprise 是一款关系型数据库服务器。SAP Enterprise Threat Detection 是一种可以检测 SAP 系统是否受到恶意攻击的产品。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，执行任意代码等。

CNVD 收录的相关漏洞包括：SAP Business Objects Business Intelligence Platform 输入验证错误漏洞、SAP Adaptive Server Enterprise SQL 注入漏洞（CNVD-2020-29747）、SAP Business Objects Business Intelligence Platform 信息泄露漏洞（CNVD-2020-29751）、SAP Adaptive Server Enterprise SQL 注入漏洞（CNVD-2020-29750）、SAP Adaptive Server Enterprise 输入验证错误漏洞、SAP Adaptive Server Enterprise 信息泄露漏洞（CNVD-2020-29753、CNVD-2020-29752）、SAP Enterprise Threat Detection 跨站脚本漏洞。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-2020-29748>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29747>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29751>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29750>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29749>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29753>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29752>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-29754>

4、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。Windows Jet Database Engine 是其中的一个数据库引擎。Windows Update Delivery Optimization（WUDO）是其中的一个 Windows 更新交付优化工具，主要用于减少因系统更新产生的网络流量。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，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Microsoft Windows Update Delivery Optimization 提权漏洞、Microsoft Windows Graphics Device Interface 信息泄露漏洞（CNVD-2020-30654）、Microsoft Windows 和 Windows Server 提权漏洞（CNVD-2020-30658）、Microsoft Windows DNS 拒绝服务漏洞、Microsoft Windows Jet Database Engine 远程代码执行漏洞（CNVD-2020-30660、CNVD-2020-30659、CNVD-2020-30662、CNVD-2020-30663）。其中，除“Microsoft Windows Graphics Device Interface 信息泄露漏洞（CNVD-2020-30654）、Microsoft Windows DNS 拒绝服务漏洞”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-2020-30657>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-30654>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-30660>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-30659>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-30658>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-30662>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-30661>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-30663>

5、rConfig 跨站请求伪造漏洞

rConfig 是一款开源的网络配置管理实用程序。本周，rConfig 被披露存在跨站请求

伪造漏洞。远程攻击者可借助特制 HTTP 请求利用该漏洞执行恶意操作。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-2020-30447>

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-2020-29732	RubyGem Rack 路径遍历漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://rubygems.org/gems/rack/versions/2.2.2
CNVD-2020-29736	多款 ESET 产品 ESET AV parsing engine 输入验证错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://support.eset.com/en/ca7387-modules-review-december-2019
CNVD-2020-29845	WordPress 权限检查绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://wpvulndb.com/vulnerabilities/10146
CNVD-2020-29871	Apple macOS Catalina CoreBluetooth 组件缓冲区溢出漏洞	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.apple.com/zh-cn/HT210919
CNVD-2020-29878	Ubiquiti Networks UniFi Video Controller 任意文件删除和 DLL 劫持漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://community.ui.com/releases/Security-advisory-bulletin-006-006/3cf6264e-e0e6-4e26-a331-1d271f84673e
CNVD-2020-30183	Samsung 移动设备缓冲区溢出漏洞 (CNVD-2020-30183)	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://security.samsungmobile.com/securityUpdate.smsb
CNVD-2020-30436	QEMU 缓冲区溢出漏洞 (CNVD-2020-30436)	高	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.qemu.org/
CNVD-2020-30440	Druva inSync Windows Client 路径遍历漏洞	高	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.druva.com/
CNVD-2020-30453	Cherokee 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://github.com/cherokee/webserver/

			commit/0d669cf4c855e8dae1e3bcd8841f863e34b10ec8
CNVD-2020-30762	多款 NETGEAR 产品缓冲区溢出漏洞 (CNVD-2020-30762)	高	厂商已发布了漏洞修复程序, 请及时关注更新: https://kb.netgear.com/000061230/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-Some-Switches-PSV-2018-0538

小结: 本周, Advantech 产品被披露存在多个漏洞, 攻击者可利用漏洞覆盖应用程序控制范围之外的文件, 获取敏感信息, 执行任意代码等。此外 Oracle、SAP、Microsoft 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, 导致拒绝服务等。另外, rConfig 被披露存在跨站请求伪造漏洞。远程攻击者可借助特制 HTTP 请求利用该漏洞执行恶意操作。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、WordPress Ultimate Member 跨站点请求伪造漏洞

验证描述

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。Ultimate Member plugin 是使用在其中的一款用于创建会员网站或在线社区的插件。

WordPress Ultimate Member 插件 2.0.38 版本中存在跨站请求伪造漏洞, 该漏洞源于 WEB 应用未充分验证请求是否来自可信用户。攻击者可利用该漏洞通过受影响客户端向服务器发送非预期的请求。

验证信息

POC 链接: <https://packetstormsecurity.com/files/152315/WordPress-Ultimate-Member-2.0.38-Cross-Site-Request-Forgery.html>

参考链接: <https://www.cnvd.org.cn/flaw/show/CNVD-2020-29847>

信息提供者

深信服科技股份有限公司

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. 研究人员发现“Apple 登录”安全漏洞：某些用户帐户可能被接管

据外媒报道，研究人员 Bhavuk Jain 在四月份发现了一个严重的「使用 Apple 登录」漏洞，该漏洞可能导致某些用户帐户被接管。值得一提的是，这个 Bug 特定于使用“通过 Apple 登录”功能且未实施其它安全措施的第三方应用。

参考链接：<https://www.ithome.com/0/490/071.htm>

2. Java 库 fastjson 被曝存“高危”远程代码执行漏洞

fastjson 当前版本为 1.2.68 发布于 3 月底，日前某安全运营中心监测到，fastjson<= 1.2.68 版本存在远程代码执行漏洞，漏洞被利用可直接获取服务器权限，漏洞等级定为“高危”。

参考链接：<https://www.ithome.com/0/490/069.htm>

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