国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 05 月 11 日-2020 年 05 月 17 日　　2020 年第 20 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 336 个，其中高危漏洞 115 个、中危漏洞 199 个、低危漏洞 22 个。漏洞平均分值为 6.16。本周收录的漏洞中，涉及 0day 漏洞 154 个（占 46%），其中互联网上出现“Zyxel NBG-418N v2 Modem 跨站请求伪造漏洞、Joomla!组件 prayercenter 'id' 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 7595 个，与上周（5514 个）环比增加 38%。

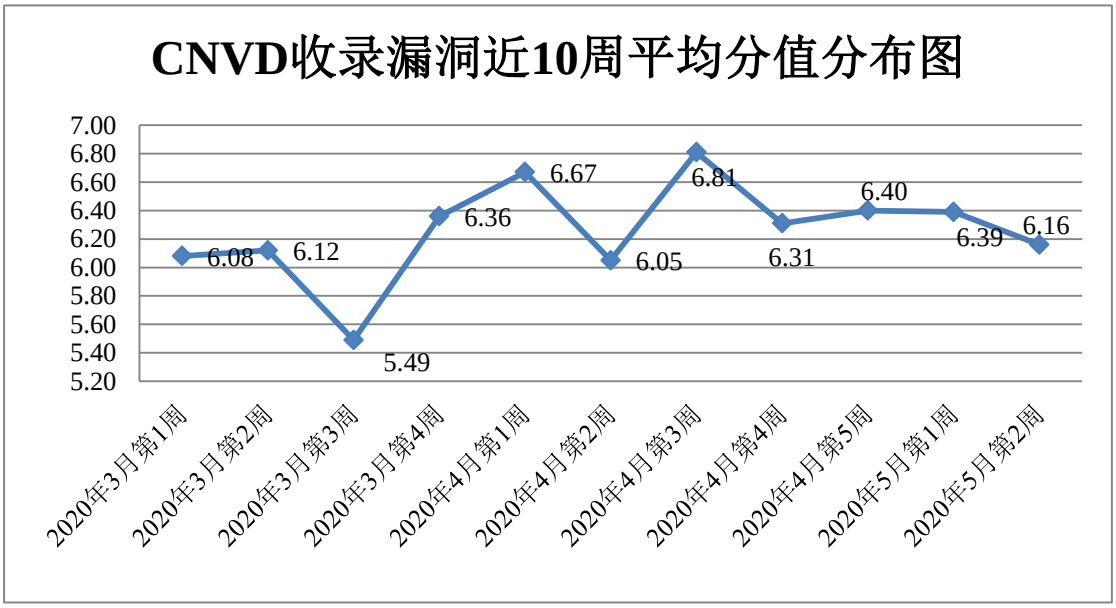

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 15 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 332 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 34 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 15 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：

湖北国昇科技有限公司、深圳市圆梦云科技有限公司、极致网络科技有限公司、哈尔滨新中新电子股份有限公司、TOM 集团有限公司、珠海金山办公软件有限公司、北京百容千域软件技术开发有限责任公司、厦门游奕网络科技有限公司、山西先启科技有限公司、龙岩讯搜网络科技有限公司、沈阳点动科技有限公司、厦门海为科技有限公司、上海丹帆网络科技有限公司、北京亚控科技发展有限公司、重庆巨泰物联网集团有限公司、南昌卓蓝科技有限公司、浙江宇视科技有限公司、陕西益和信息技术开发有限责任公司、湖南华美信息系统有限公司、昆明云涛科技有限公司、易创软件有限公司、深圳市吉祥腾达科技有限公司、成都疯马疯玛科技有限公司、廊坊市极致网络科技有限公司、宿迁鑫潮信息技术限公司、华平信息技术股份有限公司、上海展盟网络科技有限公司、杭州优云软件有限公司、北京清奇科技有限公司、成都润格无限科技有限公司、广州合优网络科技有限公司、速控云（上海）智能科技有限公司、深圳市微客互动有限公司、南京博纳睿通软件科技有限公司、上海金桥信息股份有限公司、苏州托普斯网络科技有限公司、湖南心艾网络科技有限公司、成都论之道科技有限责任公司、武汉类森科技有限公司、洛阳恒越计算机技术有限公司、环保时代网、伟创互联网络技术开发团队、子鸥科技、贴心猫、逍遥 B2C 商城系统、A4Tech、Joomla、SeaCMS、Kkcms、Advantech Co., Ltd.和 Heybbs。

本周，CNVD 发布了《Microsoft 发布 2020 年 5 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5525

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、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、华为技术有限公司、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。北京华云安信息技术有限公司、山东新潮信息技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、国瑞数码零点实验室、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、河南灵创电子科技有限公司、杭州海康威视数字技术股份有限公司、上海观安信息技术股份有限公司、北京墨云科技有限公司、山东道普测评技术有限公司、山东云天安全技术有限公司、北京圣博润高新技术股份有限公司、博智安全科技股份有限公司、北京顶象技术有限公司、北京天地和兴科技有限公司、北京长亭科技有限公司、山东华鲁科技发展股份有限公司、

成都链安科技有限公司、北京智游网安科技有限公司、安徽长泰信息安全服务有限公司、安徽风雪网络安全测评有限公司、广州美杜莎网络科技有限公司、京东云安全及其他个人白帽子向 CNVD 提交了 7595 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 6705 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
奇安信网神（补天平台）	4079	4079
斗象科技（漏洞盒子）	2272	2272
上海交大	354	354
哈尔滨安天科技集团股份有限公司	322	0
恒安嘉新(北京)科技股份公司	286	0
北京天融信网络安全技术有限公司	237	1
华为技术有限公司	206	0
新华三技术有限公司	140	0
北京神州绿盟科技有限公司	117	28
深信服科技股份有限公司	112	0
北京奇虎科技有限公司	82	25
北京启明星辰信息安全技术有限公司	60	1
中国电信集团系统集成有限责任公司	58	0
厦门服云信息科技有限公司	37	0
北京数字观星科技有限公司	20	0
中新网络信息安全股份有限公司	15	15
北京知道创宇信息技术股份有限公司	1	0

北京安信天行科技有限公司	1	1
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
北京华云安信息技术有限公司	57	57
山东新潮信息技术有限公司	49	49
远江盛邦（北京）网络安全科技股份有限公司	44	44
国瑞数码零点实验室	35	35
长春嘉诚信息技术股份有限公司	28	28
杭州迪普科技股份有限公司	25	0
内蒙古奥创科技有限公司	24	24
河南灵创电子科技有限公司	17	17
杭州海康威视数字技术股份有限公司	10	10
上海观安信息技术股份有限公司	8	8
北京墨云科技有限公司	6	6
山东道普测评技术有限公司	6	6
山东云天安全技术有限公司	6	6
北京圣博润高新技术股份有限公司	5	5
博智安全科技股份有限公司	4	4
北京顶象技术有限公司	3	3
北京天地和兴科技有限公司	3	3
北京长亭科技有限公司	3	3
山东华鲁科技发展股份有限公司	3	3
成都链安科技有限公司	2	2

北京智游网安科技有限公司	1	1
安徽长泰信息安全服务有限公司	1	1
安徽风雪网络安全测评有限公司	1	1
广州美杜莎网络科技有限公司	1	1
京东云安全	1	1
CNCERT 青海分中心	9	9
CNCERT 宁夏分中心	7	7
CNCERT 河北分中心	5	5
CNCERT 四川分中心	4	4
CNCERT 广西分中心	2	2
CNCERT 浙江分中心	1	1
个人	472	472
报送总计	9243	7595

本周漏洞按类型和厂商统计

本周，CNVD 收录了 336 个漏洞。应用程序 122 个，WEB 应用 101 个，网络设备（交换机、路由器等网络端设备）68 个，操作系统 20 个，安全产品 15 个，智能设备（物联网终端设备）8 个，数据库 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	122
WEB 应用	101
网络设备（交换机、路由器等网络端设备）	68
操作系统	20
安全产品	15
智能设备（物联网终端设备）	8
数据库	2

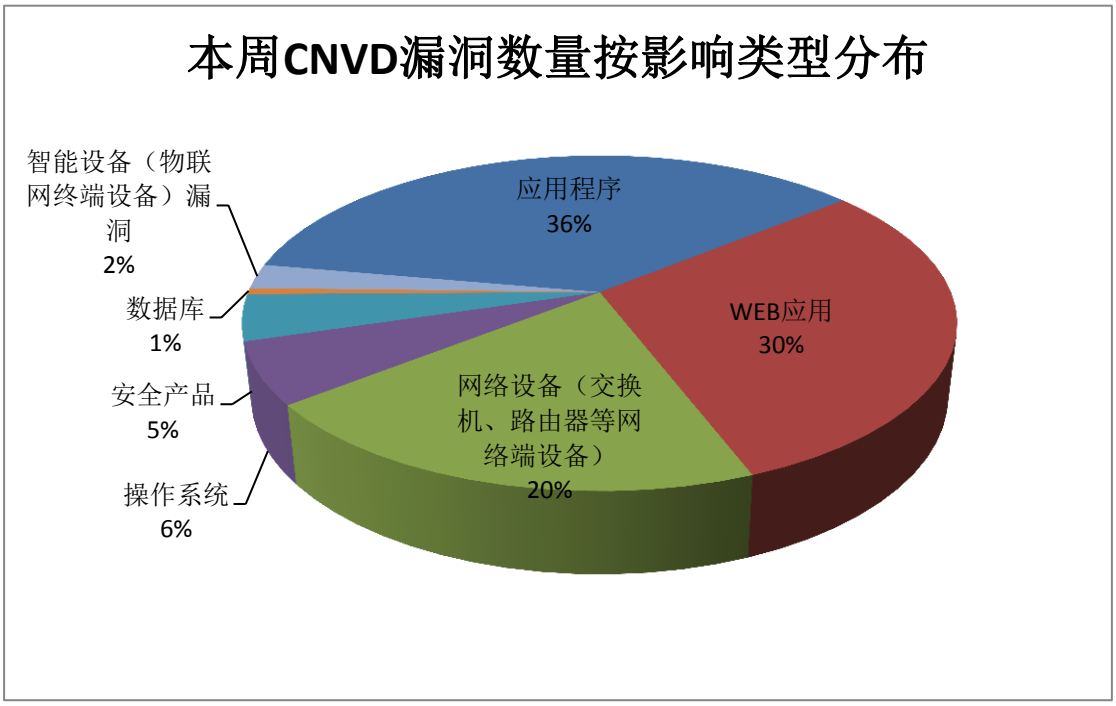

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 NETGEAR、Microsoft、JetBrains 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	NETGEAR	49	14%
2	Microsoft	19	6%
3	JetBrains	14	4%
4	Cisco	12	4%
5	IBM	12	4%
6	Zoho	11	3%
7	Oracle	10	3%
8	北京海腾时代科技有限公司	10	3%
9	Blaauw	9	3%
10	其他	190	56%

本周行业漏洞收录情况

本周，CNVD 收录了 54 个电信行业漏洞，15 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“LG 产品 MLT application intents 访问控制错误漏洞、多

款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2020-28235）”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/

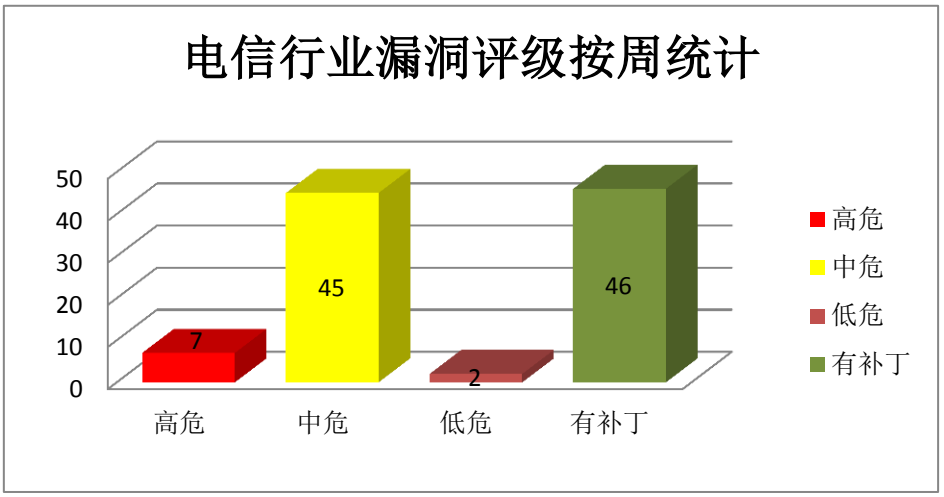

图 3 电信行业漏洞统计

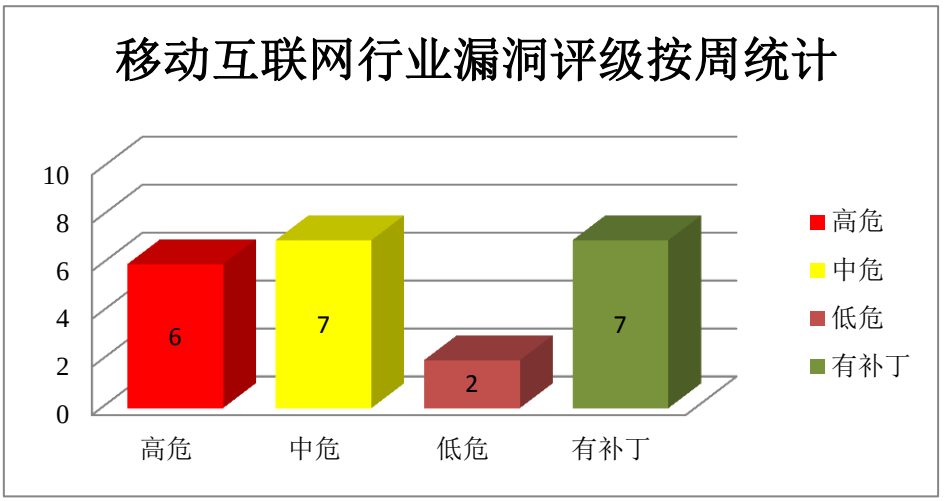

图 4 移动互联网行业漏洞统计

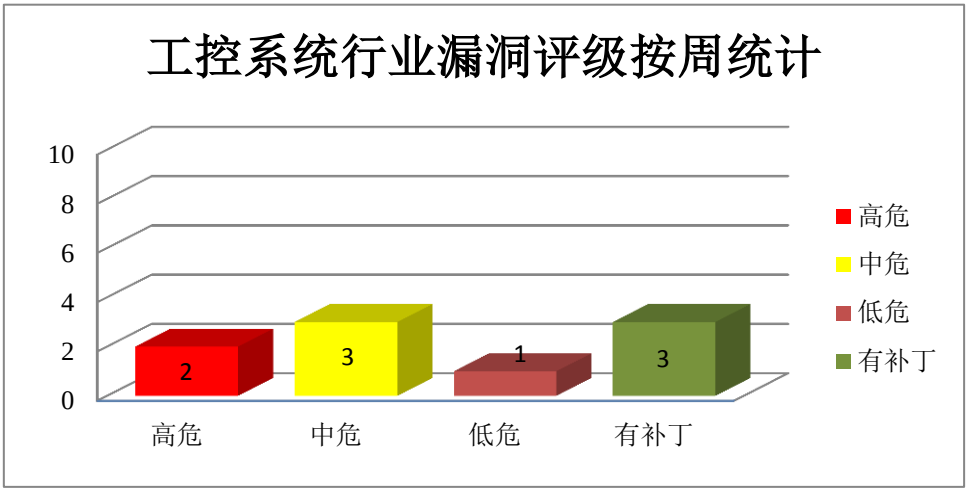

图 5 工控系统行业漏洞统计

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 Actions Http-Client 是一款轻量级的 HTTP 客户端。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。ChakraCore 是使用在 Edge 浏览器中的一个开源的 ChakraJavaScript 脚本引擎的核心部分，也可作为单独的 JavaScript 引擎使用。Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。Microsoft Word 是一套 Office 套件中的文字处理软件。Microsoft Outlook 是一套电子邮件应用程序。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，损坏内存等。

CNVD 收录的相关漏洞包括：Microsoft Actions Http-Client 信息泄露漏洞、Microsoft ChakraCore 和 Edge 远程代码执行漏洞（CNVD-2020-28238）、Microsoft Win32k 权限提升漏洞（CNVD-2020-28432）、Microsoft Windows ActiveX Installer Service 权限提升漏洞、Microsoft Windows Network Driver Interface Specification 信息泄露漏洞（CNVD-2020-28440）、Microsoft Windows Work Folder 服务权限提升漏洞、Microsoft Windows Search Indexer 权限提升漏洞、Microsoft Word 和 Microsoft Outlook 缓冲区溢出漏洞。其中，除“Microsoft Windows Work Folder 服务权限提升漏洞、Microsoft Windows Search Indexer 权限提升漏洞”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-2020-27782

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28238

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28432

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28436

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28440

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28441

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28444

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28443

2、Cisco 产品安全漏洞

Cisco Adaptive Security Appliances Software（ASA Software）是一套防火墙和网络安全平台。Cisco Firepower Threat Defense（FTD）是一套提供下一代防火墙服务的统一软件。Cisco Aironet Series Access Points Software 是一套使用在 Aironet 无线接入点设备中的软件。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身份验证，覆盖任意文件，并修改受影响设备的底层操作系统，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco Adaptive Security Appliances Software 授权问题漏洞、Cisco Firepower Threat Defense 资源管理错误漏洞（CNVD-2020-27772、CNVD-2020-27775、CNVD-2020-27774、CNVD-2020-27773）、Cisco Firepower Device Manager On-Box 输入验证错误漏洞、Cisco Firepower Threat Defense 资源管理错误漏洞（CNVD-2020-27776）、Cisco Aironet Series Access Points Software 资源管理错误漏洞。其中，除“Cisco Firepower Threat Defense 资源管理错误漏洞（CNVD-2020-27774）、Cisco Firepower Threat Defense 访问控制错误漏洞（CNVD-2020-27773）、Cisco Aironet Series Access Points Software 资源管理错误漏洞”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-2020-27770

https://www.cnvd.org.cn/flaw/show/CNVD-2020-27772

https://www.cnvd.org.cn/flaw/show/CNVD-2020-27775

https://www.cnvd.org.cn/flaw/show/CNVD-2020-27774

https://www.cnvd.org.cn/flaw/show/CNVD-2020-27773

https://www.cnvd.org.cn/flaw/show/CNVD-2020-27777

https://www.cnvd.org.cn/flaw/show/CNVD-2020-27776

https://www.cnvd.org.cn/flaw/show/CNVD-2020-27788

3、IBM 产品安全漏洞

IBM Data Risk Manager 是一款数据风险管理器。IBM WebSphere Application Server Liberty 是一款构建于 Open Liberty 项目之上的 Java 应用程序服务器。IBM UrbanCode Deploy（UCD）是一套应用自动化部署工具。IBM Cloud App Management 是一套基于

微服务架构的基础架构监控解决方案。IBM MQ 是一款消息传递中间件产品。IBM MQ Appliance 是一款用于快速部署企业级消息中间件的一体机设备。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，执行任意命令，造成拒绝服务（内存泄露）等。

CNVD 收录的相关漏洞包括：IBM Data Risk Manager 路径遍历漏洞、IBM Data Risk Manager 代码执行漏洞、IBM Data Risk Manager 操作系统命令注入漏洞、IBM Data Risk Manager 授权问题漏洞、IBM WebSphere Application Server Liberty 授权问题漏洞、IBM UrbanCode Deploy 权限提升漏洞（CNVD-2020-27949）、IBM MQ Appliance 拒绝服务漏洞（CNVD-2020-27948）、IBM Cloud App Management 信息泄露漏洞。其中，“IBM Data Risk Manager 代码执行漏洞、IBM Data Risk Manager 操作系统命令注入漏洞、IBM Data Risk Manager 授权问题漏洞”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-2020-27938
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27941
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27940
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27939
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27944
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27949
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27948
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27947

4、NETGEAR 产品安全漏洞

NETGEAR WAC505 是一款无线接入点（AP）。NETGEAR D6100 是一款无线调制解调器。NETGEAR WNDR3700 是一款无线路由器。NETGEAR R6100 是一款无线路由器。NETGEAR R9000 是一款无线路由器。NETGEAR R7800 是一款无线路由器。NETGEAR D7800 是一款无线调制解调器。NETGEAR EX2700 是一款无线网络信号扩展器。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，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2020-28140、CNVD-2020-28235、CNVD-2020-28242、CNVD-2020-28241、CNVD-2020-28244、CNVD-2020-28243、CNVD-2020-28247、CNVD-2020-28246）。其中，“多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2020-28140、CNVD-2020-28235）”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-2020-28140

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28235

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28242

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28241

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28244

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28243

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28247

https://www.cnvd.org.cn/flaw/show/CNVD-2020-28246

5、Accusoft ImageGear 缓冲区溢出漏洞（CNVD-2020-27757）

Accusoft ImageGear 是一款用于图像处理的软件开发工具包（SDK）。本周，Accusoft ImageGear 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞借助特制的 PNG 文件执行代码。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-2020-27757

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-2020-27781	PHP-Fusion SQL 注入漏洞（CNVD-2020-27781）	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/php-fusion/PHP-Fusion/issues/2308
CNVD-2020-27780	Inogard Ebiz4u 代码执行漏洞	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：http://www.ebiz4u.co.kr/
CNVD-2020-27789	Cisco Mobility Express Software 跨站请求伪造漏洞	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-mob-exp-csrf-b8tFec24
CNVD-2020-27792	JetBrains Space 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/
CNVD-2020-28050	Triangle MicroWorks SCADA Data Gateway 类型混淆漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.trianglemicroworks.com
CNVD-2020-28055	ONAP SDNC 操作系统命令注入漏洞（CNVD-2020-28055）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jira.onap.org/browse/OJSI-41

CNVD-2020-28053	Triangle MicroWorks DNP3 Outstation Libraries 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：http://www.trianglemicroworks.com/
CNVD-2020-28451	LG 产品 MLT application intents 访问控制错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lgsecurity.lge.com/security_updates.html
CNVD-2020-28463	Zoho ManageEngine OpManager SQL 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://www.manageengine.com/network-monitoring/help/read-me-complete.html
CNVD-2020-28478	Sonatype Nexus Repository Manager 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.sonatype.com/hc/en-us/articles/360044356194-CVE-2020-10204-Nexus-Repository-Manager-3-Remote-Code-Execution-2020-03-31

小结：本周，Microsoft 产品被披露存在权限提升漏洞，攻击者可利用漏洞获取敏感信息，提升权限，执行任意代码，损坏内存等。此外 Cisco、IBM、NETGEAR 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过身份验证，获取敏感信息，提升权限，执行任意命令，造成拒绝服务（内存泄露），导致缓冲区溢出或堆溢出等。另外，Accusoft ImageGear 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞借助特制的 PNG 文件执行代码。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、Joomla!组件 prayercenter 'id' SQL 注入漏洞

验证描述

Joomla!是一套开源的内容管理系统(CMS)，该系统提供 RSS 馈送、网站搜索等功能。PrayerCenter 是使用在其中的一个祷告分享组件。

Joomla!组件 prayercenter 'id'存在 SQL 注入漏洞。攻击者可利用漏洞获取数据库敏感信息。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=35501

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-28032

信息提供者

CNVD 工作组

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. 雷电 3 接口漏洞影响数百万计算机：5 分钟解锁设备，无法修复

雷电 3（Thunderbolt）接口存在缺陷，2019 年之前生产、出货的配备雷电 3 的设备都容易受到攻击。而自 2019 年后已交付的提供内核 DMA 保护的设备，也在一定程度上易受攻击。并且该漏洞不能在软件中修复，这可能直接影响未来的 USB 4 和 Thunderbolt 4 等标准，需要对芯片进行重新设计。

参考链接：https://www.freebuf.com/news/236419.html

2. 研究人员发现一系列影响 Oracle iPlanet Web Server 的漏洞

Nightwatch 网络安全研究人员于 2020 年 1 月 19 日首次发现了这些漏洞，这些问题是在企业服务器管理系统的 Web 管理控制台中发现的。被称为 CVE-2020-9315 和 CVE-2020-9314 的安全漏洞允许敏感数据公开和有限的注入攻击。

参考链接：https://www.zdnet.com/article/data-leak-phishing-security-flaws-exposed-in-oracle-iplanet-web-server/

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