国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 02 月 01 日-2021 年 02 月 07 日　　2021 年第 5 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 457 个，其中高危漏洞 163 个、中危漏洞 246 个、低危漏洞 48 个。漏洞平均分值为 5.85。本周收录的漏洞中，涉及 0day 漏洞 238 个（占 52%），其中互联网上出现“WordPress 插件 Easy Contact Form 'Name'跨站脚本漏洞、Nxlog 代码问题漏洞”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 6601 个，与上周（5712 个）环比增加 16%。

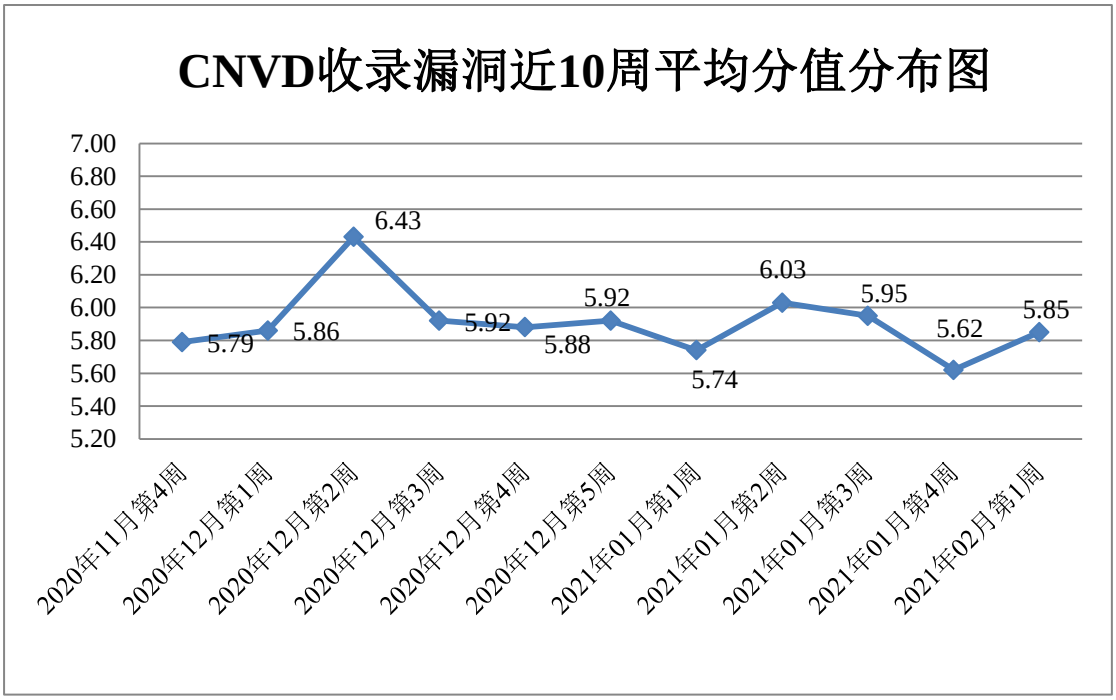

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 22 起，向基础电

信企业通报漏洞事件 14 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 154 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 26 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 31 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：

深圳创维数字技术有限公司、石家庄捷搜网络科技有限公司、上海孚盟软件有限公司、天地伟业技术有限公司、广东准度科技有限公司、厦门一指通智能科技有限公司、成都市任我行信息技术有限公司、深圳市亿图软件有限公司、正方软件股份有限公司、深圳市深智电科技有限公司、深圳市矽伟智科技有限公司、深圳市吉祥腾达科技有限公司、天津企朋科技发展有限公司、成都新线加科技有限公司、国晋信息科技有限公司、淄博闪灵网络科技有限公司、北京新东方迅程网络科技股份有限公司、上海卓赞教育科技有限公司、深圳市美科星通信技术有限公司、北京同联信息技术有限公司、深圳市大世同舟信息科技有限公司、北京飞书科技有限公司、珠海金山办公软件有限公司、昆明云涛科技有限公司、广州思迈特软件有限公司、广州同聚成电子科技有限公司、北京清大新洋科技有限公司、北京美丽时空网络科技有限公司、北京夜猫天诚网络科技有限公司、厦门佰马科技有限公司、锐捷网络股份有限公司、浙江大华技术股份有限公司、摩莎科技（上海）有限公司、上海斐讯数据通信技术有限公司、上海开始网络科技有限公司、广州网易计算机系统有限公司、成都市玖圆软件有限责任公司、北京微播视界科技有限公司、瑞安市优博科技有限公司、维沃移动通信有限公司、湖北点点点科技有限公司、普联技术有限公司、安徽名流健康管理有限公司、深圳华望技术有限公司、济南亘安信息技术有限公司、北京兆信信息技术股份有限公司、沈阳盘古网络技术有限公司、成都时代汇创科技有限公司、深圳好生意网络工作室、深圳市筷云信息科技股份有限公司、长沙友点软件科技有限公司、江苏汉思未来信息科技有限公司、广州市贝佳软件开发有限公司、河北云在信息技术服务有限公司、深圳市河辰通讯技术有限公司、三星（中国）投资有限公司、上海商派网络科技有限公司、深圳市维君瑞科技有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、上海智休信息科技有限公司、北京三快云计算有限公司、北京学而思教育科技有限公司、北京猿力教育科技有限公司、上海互盾信息科技有限公司、新东方教育科技集团有限公司、北京万友映力科技有限公司、湖北京伦集团股份有限公司、北京百家互联科技有限公司、北京爱奇艺科技有限公司、广州合优网络科技有限公司、上海喜马拉雅科技有限公司、广州拓波软件科技有限公司、北京百家视联科技有限公司、杭州网易质云科技有限公司、北京乐博乐博教育科技有限公司、扎兰屯市爱发网络科技有限公司、济南有人物联网技术有限公司、上海纵之格科技有限公司、广州红帆科技有限公司、北京小米科技有限责任公司、上海国云信息科技有限公司、聪投（北京）信息技术有限公司、北京通达信科科技有限公司、深圳市阿卡索

资讯股份有限公司、常熟市畅享计算机信息技术有限公司、深圳市圆梦云科技有限公司、屏通科技（上海）有限公司、商派软件有限公司、佛山市杜特软件科技有限公司、北京火绒网络科技有限公司、沈阳优诺科技有限公司、广东凯格科技有限公司、广州馨香日用化工有限公司、杭州智聪网络科技有限公司、湖北淘码千维信息科技有限公司、厦门科拓通讯技术股份有限公司、联奕科技股份有限公司、网易公司、无锡信捷电气股份有限公司、杭州橙诺科技有限公司、二六三网络通信股份有限公司、方正证券股份有限公司、屏通科技股份有限公司、上海赛连信息科技有限公司、苏州酷曼软件技术有限公司、阿里巴巴集团安全应急响应中心、河北欧润天腾云梦吧网络工作室、若依、海海软件、英飞拓(Infinova)、海洋 CMS、Bandisoft、WMCMS、HsyCMS、McAfee, LLC、seacms、MinIO, Inc.、Adobe、AdGuard、Open Source Matters、ShuipFCMS、NetSarang、VideoLAN、yzmcms 和 xiycms。

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、深信服科技股份有限公司、新华三技术有限公司、北京启明星辰信息安全技术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、上海犀点意象网络科技有限公司、山东云天安全技术有限公司、国瑞数码零点实验室、安徽长泰信息安全服务有限公司、北京山石网科信息技术有限公司、北京天地和兴科技有限公司、河南灵创电子科技有限公司、北京华云安信息技术有限公司、山东华鲁科技发展股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、上海纽盾科技股份有限公司、京东云安全、河南信安世纪科技有限公司、新疆海狼科技有限公司、广州市蓝爵计算机科技有限公司、杭州安信检测技术有限公司、贵州多彩宝互联网服务有限公司、北京惠而特科技有限公司、北京零零信安科技有限公司、深圳市魔方安全科技有限公司、北京信联科汇科技有限公司、北京远禾科技有限公司、奇安信-工控安全实验室、内蒙古奥创科技有限公司、平安银河实验室、海南神州希望网路有限公司、北京圣博润高新技术股份有限公司、上海峭函信息科技有限公司、江苏保旺达软件技术有限公司、武汉明嘉信信息安全检测评估有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、广西塔易信息技术有限公司、广州安亿信软件科技有限公司、泽鹿安全、福建省海峡信息技术有限公司、上海市信息安全测评认证中心、北京时代新威信息技术有限公司、国网山东省电力公司、北京机沃科技有限公司、北京明朝万达科技股份有限公司（安元实验室）、北京智游网安科技有限公司、上海观安信息技术股份有限公司及其他个人白帽子向 CNVD 提交了 6601 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 3833 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）	1868	1868
上海交大	1191	1191
奇安信网神（补天平台）	763	763
北京天融信网络安全技术有限公司	345	8
哈尔滨安天科技集团股份有限公司	296	296
深信服科技股份有限公司	162	162
新华三技术有限公司	137	137
北京启明星辰信息安全技术有限公司	117	1
华为技术有限公司	115	115
北京神州绿盟科技有限公司	115	11
北京奇虎科技有限公司	94	94
北京数字观星科技有限公司	43	43
中国电信集团系统集成有限责任公司	23	23
中国电信股份有限公司网络安全产品运营中心	20	20
北京知道创宇信息技术股份有限公司	5	5
恒安嘉新(北京)科技股份公司	4	3
南京众智维信息科技有限公司	324	324
上海犀点意象网络科技有限公司	246	246
山东云天安全技术有限公司	145	145
国瑞数码零点实验室	125	125
安徽长泰信息安全服务有限公司	59	59
北京山石网科信息技术有限公司	54	54
北京天地和兴科技有限公司	43	43
河南灵创电子科技有限公司	36	36
北京华云安信息技术有限公司	27	27
山东华鲁科技发展股份有限公司	21	21
远江盛邦（北京）网络安全科技股份有限公司	16	16

上海纽盾科技股份有限公司	11	11
京东云安全	10	10
河南信安世纪科技有限公司	9	9
新疆海狼科技有限公司	8	8
广州市蓝爵计算机科技有限公司	8	8
杭州安信检测技术有限公司	7	7
贵州多彩宝互联网服务有限公司	6	6
北京惠而特科技有限公司	6	6
北京零零信安科技有限公司	6	6
深圳市魔方安全科技有限公司	5	5
北京信联科汇科技有限公司	5	5
北京远禾科技有限公司	5	5
奇安信-工控安全实验室	4	4
内蒙古奥创科技有限公司	3	3
平安银河实验室	3	3
海南神州希望网路有限公司	3	3
北京圣博润高新技术股份有限公司	3	3
北京华顺信安科技有限公司	2	0
上海崤函信息科技有限公司	2	2
江苏保旺达软件技术有限公司	2	2
武汉明嘉信信息安全检测评估有限公司	2	2
北京云科安信科技有限公司（Seraph 安全实验室）	2	2
广西塔易信息技术有限公司	2	2
广州安亿信软件科技有限公司	2	2
泽鹿安全	2	2
福建省海峡信息技术有限公司	2	2
上海市信息安全测评认证中心	2	2
北京时代新威信息技术有限公司	2	2
国网山东省电力公司	1	1
北京机沃科技有限公司	1	1
北京明朝万达科技股份有限公司（安元实验室）	1	1

北京智游网安科技有限公司	1	1
上海观安信息技术股份有限公司	1	1
CNCERT 河北分中心	24	24
CNCERT 青海分中心	8	8
CNCERT 青海分中心	8	8
CNCERT 贵州分中心	6	6
CNCERT 山西分中心	3	3
CNCERT 四川分中心	2	2
CNCERT 西藏分中心	2	2
个人	585	585
报送总计	7161	6601

本周漏洞按类型和厂商统计

本周，CNVD 收录了 457 个漏洞。应用程序 234 个，WEB 应用 116 个，网络设备（交换机、路由器等网络端设备）34 个，操作系统 31 个，安全产品 22 个，数据库 13 个，工业控制系统 5 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	234
WEB 应用	116
网络设备（交换机、路由器等网络端设备）	34
操作系统	31
安全产品	22
数据库	13
工业控制系统	5
智能设备（物联网终端设备）	2

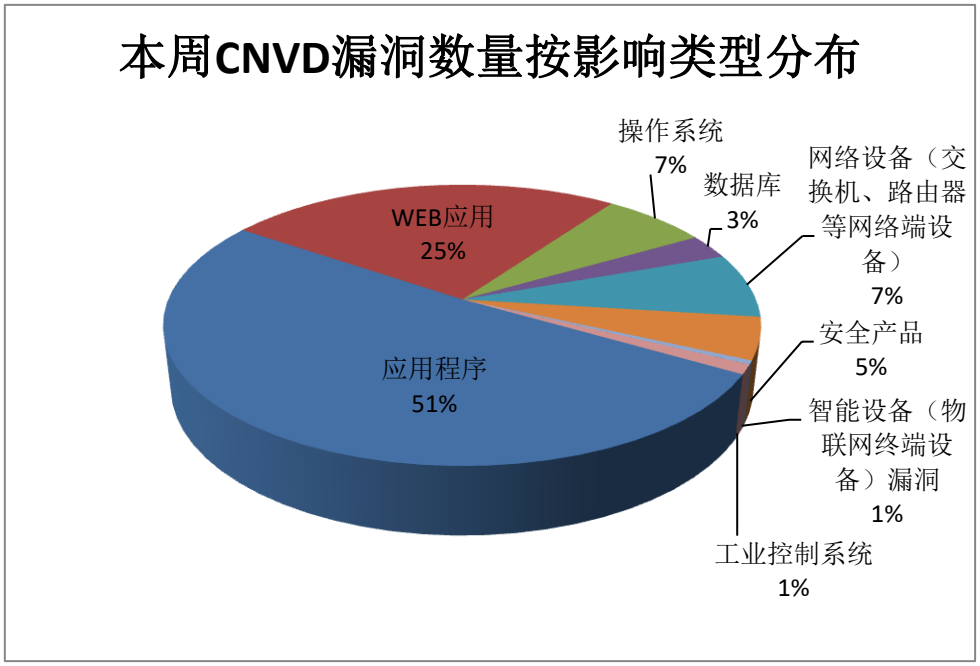

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、北京海腾时代科技有限公司、Trend Micro 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	Oracle	74	16%
2	北京海腾时代科技有限公司	21	5%
3	Trend Micro	20	4%
4	深圳市腾讯计算机系统有限公司	17	4%
5	Microsoft	17	4%
6	IBM	14	3%
7	Cisco	14	3%
8	Google	13	3%
9	JetBrains	13	3%
10	其他	254	55%

本周行业漏洞收录情况

本周，CNVD 收录了 31 个电信行业漏洞，22 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2021-08834）、Cisco IOS XR 拒绝服务漏洞（CNVD-2021-09297）、Google Android Framework 权限提升漏洞（CNVD-2021-09487）”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/

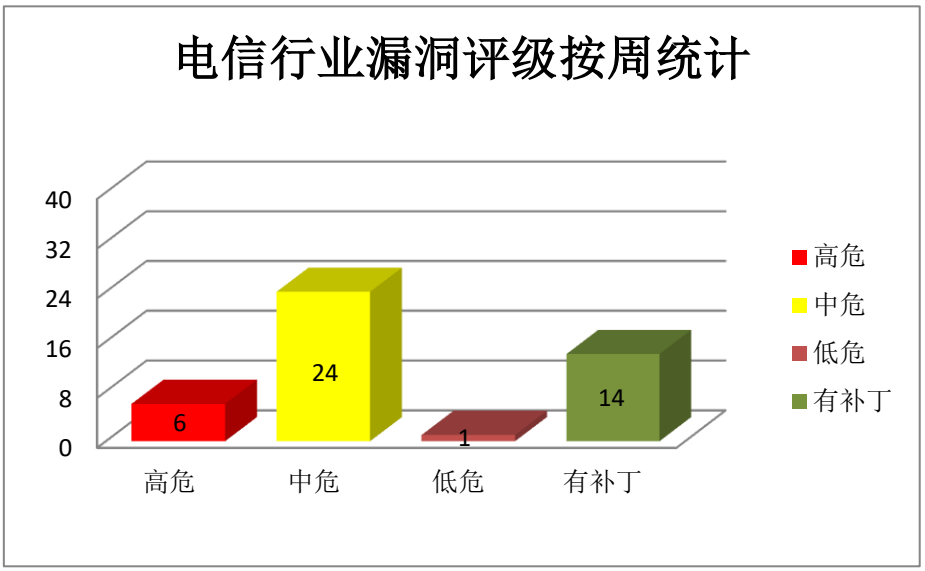

图 3 电信行业漏洞统计

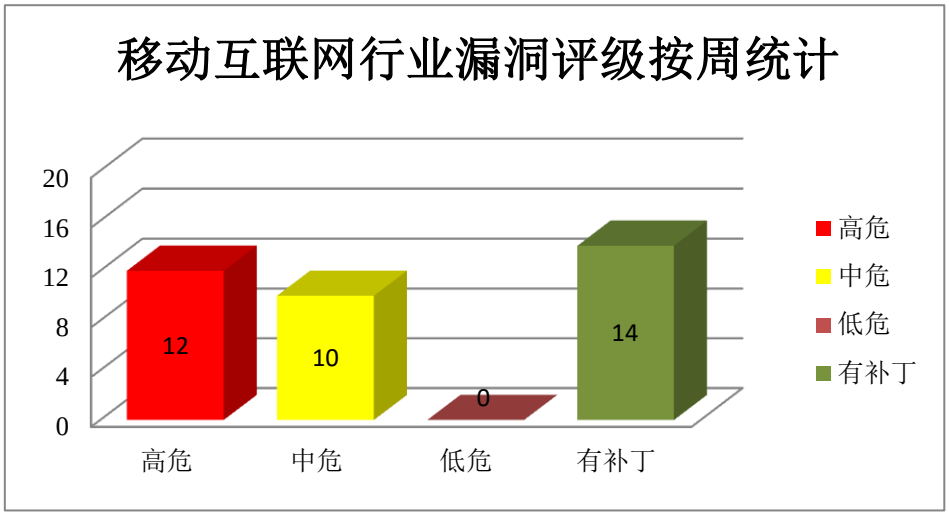

图 4 移动互联网行业漏洞统计

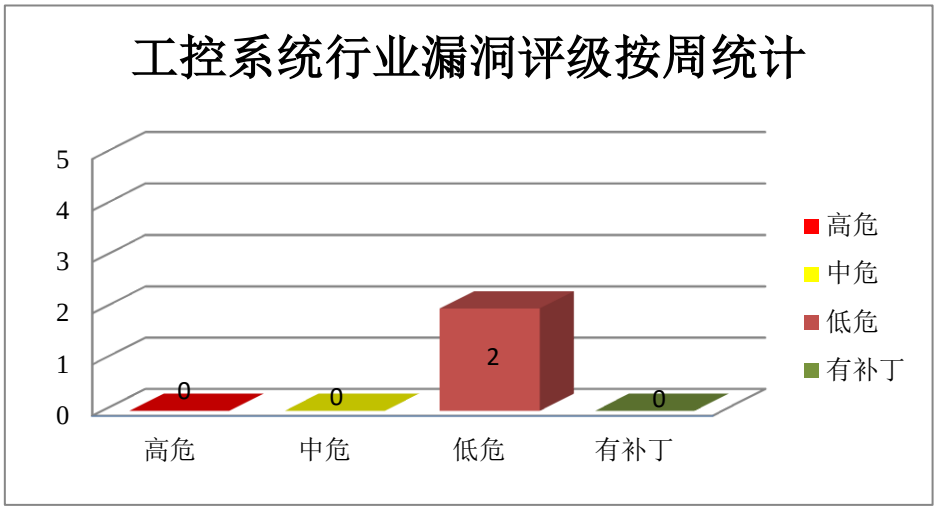

图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

Oracle E-Business Suite（电子商务套件）是美国甲骨文（Oracle）公司的一套全面集成式的全球业务管理软件。本周，上述产品被披露存在授权问题漏洞，攻击者可利用该漏洞影响机密性和完整性。

CNVD 收录的相关漏洞包括：Oracle E-Business Suite 授权问题漏洞（CNVD-2021-08445、CNVD-2021-08444、CNVD-2021-08448、CNVD-2021-08447、CNVD-2021-08452、CNVD-2021-08451、CNVD-2021-08450、CNVD-2021-08449）。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-2021-08445
https://www.cnvd.org.cn/flaw/show/CNVD-2021-08444
https://www.cnvd.org.cn/flaw/show/CNVD-2021-08448
https://www.cnvd.org.cn/flaw/show/CNVD-2021-08447
https://www.cnvd.org.cn/flaw/show/CNVD-2021-08452
https://www.cnvd.org.cn/flaw/show/CNVD-2021-08451
https://www.cnvd.org.cn/flaw/show/CNVD-2021-08450
https://www.cnvd.org.cn/flaw/show/CNVD-2021-08449

2、Google 产品安全漏洞

Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在权限提升漏洞，攻击者可利用

漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android Framework 权限提升漏洞（CNVD-2021-09483、CNVD-2021-09482、CNVD-2021-09481、CNVD-2021-09486、CNVD-2021-09485、CNVD-2021-09484、CNVD-2021-09488、CNVD-2021-09487）。其中，“Google Android Framework 权限提升漏洞（CNVD-2021-09482、CNVD-2021-09486、CNVD-2021-09485、CNVD-2021-09487）”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-2021-09483

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09482

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09481

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09486

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09485

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09484

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09488

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09487

3、Cisco 产品安全漏洞

Cisco IOS XR 软件是用于服务提供商网络的模块化和完全分布式的网络操作系统。Cisco Managed Services Accelerator (MSX)是一个多租户、多服务、云原生的服务创建和交付平台，可帮助服务提供商快速、轻松且经济高效地为企业客户开发和交付托管服务。Cisco SD-WAN vEdge 是美国思科（Cisco）公司的是一款路由器。Cisco Data Center Network Manager (DCNM)是 Cisco 的一套数据中心网络管理器，可对网络进行多协议管理，并对交换机的运行状况和性能提供故障排除功能。Cisco StarOS 是一套路由器操作系统，可控制整个系统逻辑，可控制进程和 CLI。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，删除文件系统上的任意文件，导致拒绝服务。

CNVD 收录的相关漏洞包括：Cisco IOS XR 拒绝服务漏洞（CNVD-2021-09295、CNVD-2021-09297、CNVD-2021-09296）、Cisco Managed Services Accelerator 拒绝服务漏洞、Cisco IOS XR 信息泄露漏洞、Cisco SD-WAN Software 信息泄露漏洞、Cisco Data Center Network Manager 路径遍历漏洞（CNVD-2021-09309）、Cisco StarOS 拒绝服务漏洞（CNVD-2021-09312）。其中，“Cisco IOS XR 拒绝服务漏洞（CNVD-2021-09297、CNVD-2021-09296）、Cisco Data Center Network Manager 路径遍历漏洞（CNVD-2021-09309）”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-2021-09295

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09298

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09297

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09296

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09299

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09304

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09309

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09312

4、Microsoft 产品安全漏洞

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。Microsoft Windows Hyper-V 是美国微软（Microsoft）公司的一款可提供硬件虚拟化的工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以提升的权限执行代码等。

CNVD 收录的相关漏洞包括：Microsoft Windows Codecs 远程代码执行漏洞、Microsoft Windows 内核映像权限提升漏洞、Microsoft Windows 内核模式驱动程序权限提升漏洞、Microsoft Windows Hyper-V 权限提升漏洞（CNVD-2021-08829）、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2021-08834）、Microsoft Windows Installer 权限提升漏洞（CNVD-2021-08833）、Microsoft Windows WER 权限提升漏洞、Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2021-08838）。其中，除“Microsoft Windows Codecs 远程代码执行漏洞、Microsoft Windows WER 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-2021-08826

https://www.cnvd.org.cn/flaw/show/CNVD-2021-08831

https://www.cnvd.org.cn/flaw/show/CNVD-2021-08830

https://www.cnvd.org.cn/flaw/show/CNVD-2021-08829

https://www.cnvd.org.cn/flaw/show/CNVD-2021-08834

https://www.cnvd.org.cn/flaw/show/CNVD-2021-08833

https://www.cnvd.org.cn/flaw/show/CNVD-2021-08837

https://www.cnvd.org.cn/flaw/show/CNVD-2021-08838

5、EasyCMS 跨站请求伪造漏洞（CNVD-2021-09498）

EasyCMS 是轻量级可扩展的开源内容管理程序，遵循 Apache2 开源协议发布。本周，EasyCMS 被披露存在跨站请求伪造漏洞。攻击者可通过 index.php?s=/admin/rbacuser/insert/navTabId/rbacuser/callbackType/closeCurrent 利用该漏洞添加管理员帐户。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-2021-09498

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-2021-07932	IBM Security Guardium 不当访问控制漏洞	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/6408630
CNVD-2021-08013	Oracle Fusion Middleware Coherence 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://www.oracle.com/security-alerts/cpujan2021.html
CNVD-2021-08148	Veritas NetBackup 和 Veritas NetBackup Opscenter 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.veritas.com/content/support/en_US/security/VTS20-016
CNVD-2021-08147	Veritas Desktop and Laptop Option 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.veritas.com/content/support/en_US/security/VTS20-012
CNVD-2021-08543	Trend Micro InterScan Web Security Virtual Appliance 命令注入漏洞（CNVD-2021-08543）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://success.trendmicro.com/solution/000281954
CNVD-2021-08557	Trend Micro OfficeScan XG SP1 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://success.trendmicro.com/solution/000263633
CNVD-2021-09493	QNAP Systems Helpdesk 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.qnap.com/zh-tw/security-advisory/qsa-20-08
CNVD-2021-09795	JetBrains YouTrack 服务器端模板注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/
CNVD-2021-09803	TerraMaster TOS 动态类方法调用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://help.terra-master.com/TOS/view/
CNVD-2021-09801	ThinkJS 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://github.com/thinkjs/thinkjs

小结：本周，Oracle 产品被披露存在授权问题漏洞，攻击者可利用该漏洞影响机密性和完整性。此外，Google、Cisco、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，删除文件系统上的任意文件，以提升的权限执行代码，导致拒绝服务等。另外，EasyCMS 被披露存在跨站请求伪造漏洞。攻击者可通过 index.php?s=/admin/rbacuser/insert/navTabId/rbacuser/callbackType/closeCurrent 利用该漏洞添加管理员帐户。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 插件 Easy Contact Form 'Name'跨站脚本漏洞

验证描述

WordPress 是基于 PHP 语言开发的博客平台，可以用于在支持 PHP 和 MySQL 数据库的服务器上架设网站，也可当做一个内容管理系统（CMS）。

WordPress 插件 Easy Contact Form 'Name'跨站脚本漏洞。攻击者可利用该漏洞向 Web 页面中注入 JavaScript 代码。

验证信息

POC 链接：https://packetstormsecurity.com/files/160958/WordPress-Easy-Contact-Form-1.1.7-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-09816

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、思科发现其小型企商业 VPN 路由器的严重漏洞，或将影响在家工作的人员

攻击者可利用这些漏洞以 root 用户身份执行任意代码。思科已经解决了这些关键漏洞，目前尚未发现这些漏洞被利用的痕迹，呼吁大家及时更新小型商业 VPN 路由器系列中 RV160,RV160W, RV260, RV260P,和 RV260W 这些型号的补丁。

参考链接：https://thehackernews.com/2021/01/new-docker-container-escape-bug-affects.html

2、SolarWinds 软件被发现了 3 个新的严重安全漏洞

网络安全研究人员披露了三个严重的安全漏洞，这些漏洞影响了 SolarWinds 产品，其中最严重的漏洞可能已被利用来实现具有更高特权的远程代码执行。

参考链接：https://thehackernews.com/2021/02/3-new-severe-security-vulnerabilities.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