国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 03 月 01 日-2021 年 03 月 07 日　　2021 年第 9 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 488 个，其中高危漏洞 196 个、中危漏洞 244 个、低危漏洞 48 个。漏洞平均分值为 6.11。本周收录的漏洞中，涉及 0day 漏洞 208 个（占 43%），其中互联网上出现“UltimateKode Neo Billing 跨站脚本漏洞、PHPSHE SQL 注入漏洞（CNVD-2021-14156）”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 6101 个，与上周（4894 个）环比增加 25%。

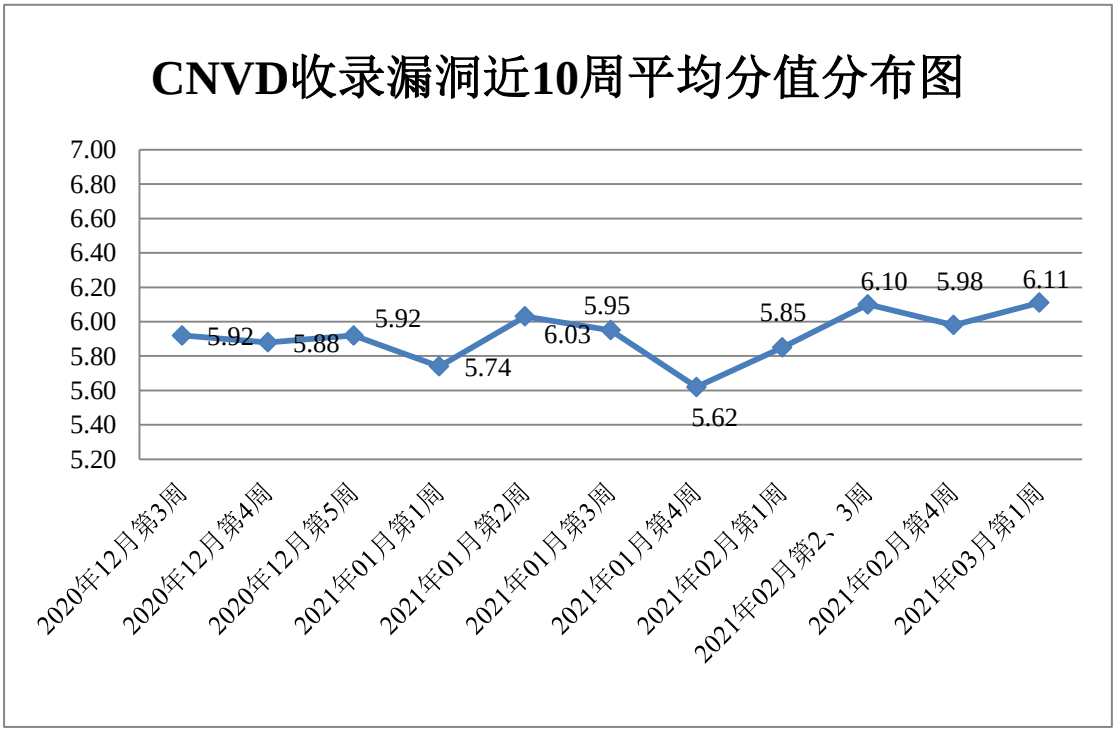

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 22 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 504 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 59 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 27 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：

广州市奥威亚电子科技有限公司、三菱电机自动化（中国）有限公司、北京信安世纪科技股份有限公司、杭州启博海纳数字科技有限公司、上海艾泰科技有限公司、上海安硕信息技术股份有限公司、淄博邦诺网络科技有限公司、深圳神州通达网络技术有限公司、哈尔滨伟成科技有限公司、深圳维盟科技股份有限公司、北京伟联科技有限公司、广州市璐华计算机科技有限公司、深圳市迅雷网络技术有限公司、网旭科技有限公司、茉柏枘（上海）软件科技有限公司、厦门优莱柏网络科技有限公司、淄博闪灵网络科技有限公司、北京爱奇艺科技有限公司、民生证券股份有限公司、国开证券股份有限公司、东兴证券股份有限公司、华龙证券股份有限公司、北京新东方迅程网络科技股份有限公司、中国银河证券股份有限公司、江海证券有限公司、北京亚控科技发展有限公司、速达软件技术（广州）有限公司、福建智度科技有限公司、雷神（武汉）信息技术有限公司、北京海腾时代科技有限公司、山东万岳信息科技有限公司、厦门四信通信科技有限公司、中电鸿信信息科技有限公司、深圳市明源云科技有限公司、唐山市柳林自动化设备有限公司、华金证券股份有限公司、天风证券股份有限公司、大同证券有限责任公司、上海迈微软件科技有限公司、甬兴证券有限公司、蓝信移动（北京）科技有限公司、深圳市汇佳互联科技有限公司、万兴科技集团股份有限公司、上海享互网络科技有限公司、爱建证券有限责任公司、长城国瑞证券有限公司、库卡（KUKA）机器人有限公司、北京 1039 科技发展有限公司、深圳市管家婆网络服务有限公司、上海牛迈网络科技有限公司、四川思途智旅软件有限公司、中山证券有限责任公司、华鑫证券有限责任公司、华西证券股份有限公司、上海嵩恒网络科技股份有限公司、中兴通讯股份有限公司、山西牛酷信息科技有限公司、微软(中国)有限公司、上海泛微网络科技股份有限公司、海南赞赞网络科技有限公司、北京壹零叁玖科技发展有限公司、北京玛格泰克科技发展有限公司、湖北淘码千维信息科技有限公司、北京坤豆科技有限公司、南京奇炫欢享网络技术有限公司、上海罗湖斯自动化技术有限公司、上海穆云智能科技有限公司、湘财证券股份有限公司、深圳市网旭科技有限公司、苹果电子产品商贸(北京)有限公司、东莞证券股份有限公司、上海互盾信息科技有限公司、德邦证券股份有限公司、深圳市傲冠软件股份有限公司、大唐电信科技股份有限公司、锐捷网络股份有限公司、北京易普拉格科技股份有限公司、川财证券有限责任公司、浙江大华技术股份有限公司、四川清和科技有限公司、厦门书生企友通科技有限公司、珠海金山办公软件有限公司、任子行网络技术股份有限公司、广州网易计算机系统有限公司、佛山市贝密信息科技有限公司、

上海装盟信息科技有限公司、北京九思易自动化软件有限公司、杭州荷花软件有限公司、普联技术有限公司、深圳市腾讯计算机系统有限公司、中天证券股份有限公司、华融证券股份有限公司、大庆紫金桥软件技术有限公司、万联证券股份有限公司、华福证券有限责任公司、南大傲拓科技股份有限公司、用友网络科技股份有限公司、常州天健管理咨询有限公司、湖南一唯信息科技有限公司、北京风行在线技术有限公司、北京朗新天霁软件技术有限公司、万户科技、京东安全应急响应中心、阿里巴巴集团安全应急响应中心、安信证券、台湾威纶通科技、东八区品牌创意、米酷资源网、上海互盾、深圳好生意网络工作室、易如意、沪江、狂雨小说 cms 、发货 100、Bandicam Company 、WordPress、SEACMS、Domotz、JFinalOA、SIYUCMS、Nitro、ZengCMS、yycms、Splashtop 和 kitecms。

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、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、华为技术有限公司、厦门服云信息科技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、山东云天安全技术有限公司、上海犀点意象网络科技有限公司、山东泽鹿安全技术有限公司、北京信联科汇科技有限公司、安徽长泰信息安全服务有限公司、北京天地和兴科技有限公司、河南灵创电子科技有限公司 、贵州多彩宝互联网服务有限公司、北京华云安信息技术有限公司、北京山石网科信息技术有限公司、武汉明嘉信信息安全检测评估有限公司、河南信安世纪科技有限公司、杭州迪普科技股份有限公司、北京顶象技术有限公司、国瑞数码零点实验室、山东华鲁科技发展股份有限公司、北京远禾科技有限公司、星云博创科技有限公司、北京惠而特科技有限公司、福建省海峡信息技术有限公司、上海峭函信息科技有限公司、内蒙古奥创科技有限公司、北京华顺信安科技有限公司、联想全球安全实验室、上海纽盾科技股份有限公司、广州市蓝爵计算机科技有限公司、广州安亿信软件科技有限公司、河南省鼎信信息安全等级测评有限公司、吉林谛听信息技术有限公司、上海匡创信息技术有限公司、北京智游网安科技有限公司、北京安帝科技有限公司、北京君云天下科技有限公司、北京长亭科技有限公司、江苏保旺达软件技术有限公司、内蒙古洞明科技有限公司、山石网科通信技术股份有限公司、上海市信息安全测评认证中心、上海上讯信息技术股份有限公司、深圳市魔方安全科技有限公司、四川哨兵信息科技有限公司、工业信息安全(四川)创新中心有限公司及其他个人白帽子向 CNVD 提交了 6101 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 4450 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）	2972	2972
斗象科技（漏洞盒子）	898	898
上海交大	580	580
哈尔滨安天科技集团股份有限公司	267	0
北京天融信网络安全技术有限公司	252	2
北京神州绿盟科技有限公司	185	79
华为技术有限公司	121	0
新华三技术有限公司	118	0
厦门服云信息科技有限公司	111	0
深信服科技股份有限公司	108	0
北京数字观星科技有限公司	69	0
北京启明星辰信息安全技术有限公司	53	1
中国电信股份有限公司网络安全产品运营中心	27	7
中国电信集团系统集成有限责任公司	16	16
北京知道创宇信息技术股份有限公司	7	1
南京众智维信息科技有限公司	149	149
山东云天安全技术有限公司	97	97
上海犀点意象网络科技有限公司	58	58
山东泽鹿安全技术有限公司	50	50
北京信联科汇科技有限公司	39	39
安徽长泰信息安全服务有限公司	23	23
北京天地和兴科技有限公司	31	31
河南灵创电子科技有限公司	28	28
贵州多彩宝互联网服务有限	26	26

公司		
北京华云安信息技术有限公司	25	25
北京山石网科信息技术有限公司	21	21
武汉明嘉信信息安全检测评估有限公司	19	19
河南信安世纪科技有限公司	18	18
杭州迪普科技股份有限公司	16	0
北京顶象技术有限公司	13	13
国瑞数码零点实验室	13	13
山东华鲁科技发展股份有限公司	12	12
北京远禾科技有限公司	7	7
星云博创科技有限公司	7	7
北京惠而特科技有限公司	5	5
福建省海峡信息技术有限公司	5	5
上海崤函信息科技有限公司	5	5
内蒙古奥创科技有限公司	5	5
北京华顺信安科技有限公司	4	0
联想全球安全实验室	3	3
上海纽盾科技股份有限公司	3	3
广州市蓝爵计算机科技有限公司	2	2
广州安亿信软件科技有限公司	2	2
河南省鼎信信息安全等级测评有限公司	2	2
吉林谛听信息技术有限公司	2	2
上海匡创信息技术有限公司	2	2
北京智游网安科技有限公司	1	1
北京安帝科技有限公司	1	1
北京君云天下科技有限公司	1	1

北京长亭科技有限公司	1	1
江苏保旺达软件技术有限公司	1	1
内蒙古洞明科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
上海市信息安全测评认证中心	1	1
上海上讯信息技术股份有限公司	1	1
深圳市魔方安全科技有限公司	1	1
四川哨兵信息科技有限公司	1	1
工业信息安全(四川)创新中心有限公司	1	1
CNCERT 西藏分中心	6	6
CNCERT 青海分中心	4	4
CNCERT 四川分中心	3	3
个人	848	848
报送总计	7349	6101

本周漏洞按类型和厂商统计

本周，CNVD 收录了 488 个漏洞。应用程序 278 个，WEB 应用 115 个，网络设备（交换机、路由器等网络端设备）38 个，操作系统 32 个，安全产品 12 个，智能设备（物联网终端设备）11 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	278
WEB 应用	115
网络设备（交换机、路由器等网络端设备）	38
操作系统	32
安全产品	12
智能设备（物联网终端设备）	11
数据库	2

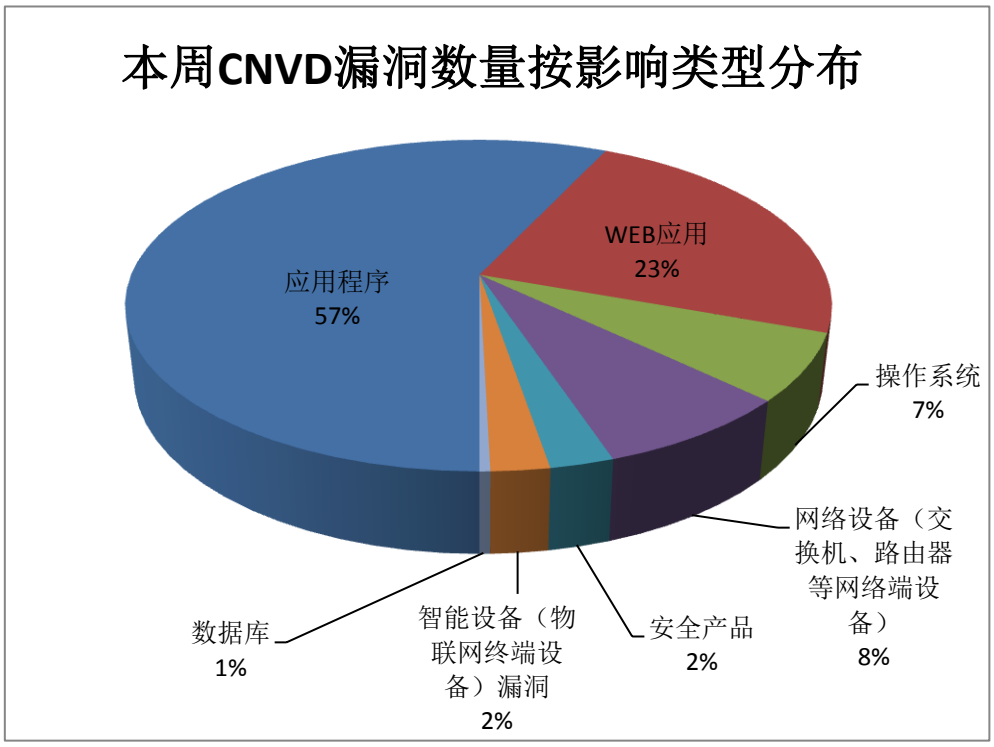

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、HCL、Mozilla 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	40	8%
2	HCL	27	6%
3	Mozilla	18	4%
4	Adobe	17	4%
5	DELL	16	3%
6	Aruba Networks	11	2%
7	Mofi Network	10	2%
8	SoftMaker	10	2%
9	湖北淘码千维信息科技有限公司	10	2%
10	其他	329	67%

本周行业漏洞收录情况

本周，CNVD 收录了 25 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，“ Cisco Nexus 9000 系列交换机拒绝服务漏洞（CNVD-2021-14793）、Mofi Network MOFI4500-4GXeLTE 未授权 RCE 漏洞、Mofi Network MOFI4500-4GXeLTE 认证绕过漏洞、Google Android System 权限提升漏洞（CNVD-2021-

13687）、Google Android System 远程代码执行漏洞（CNVD-2021-13692）”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/

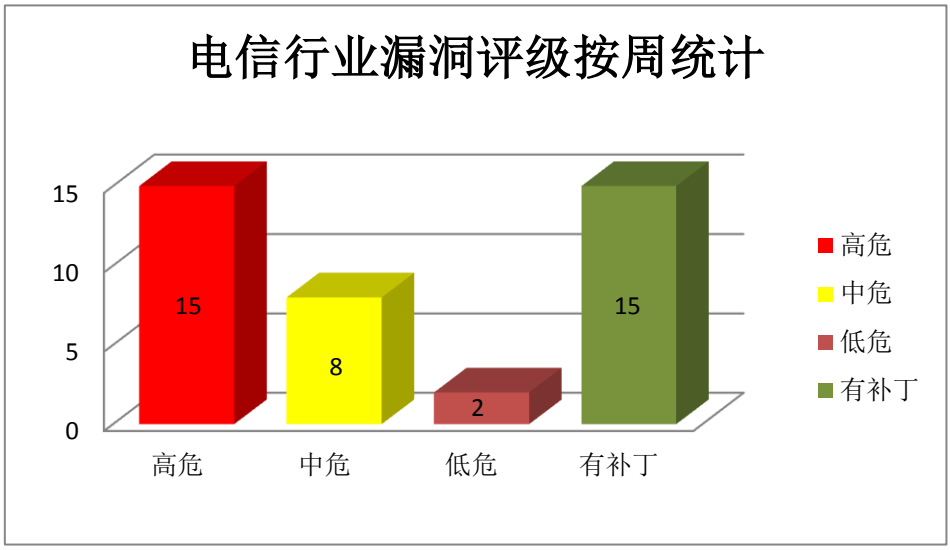

图 3 电信行业漏洞统计

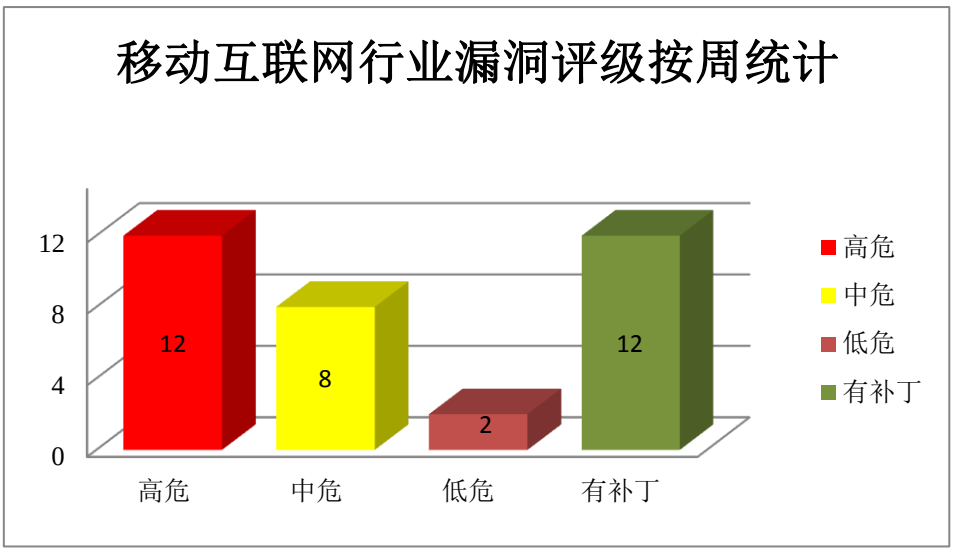

图 4 移动互联网行业漏洞统计

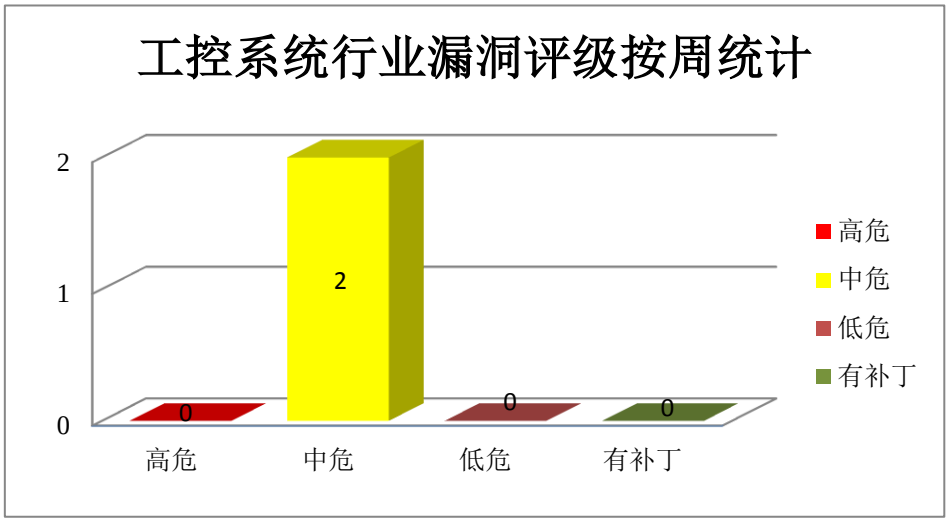

图 5 工控系统行业漏洞统计

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、DELL 产品安全漏洞

Dell EMC PowerScale OneFS 是一款由 API 驱动的文件系统。Dell EMC Isilon OneFS 和 Dell EMC PowerScale OneFS 都是美国戴尔（DELL）公司的一套适用于非结构化数据的横向扩展存储系统。Dell EMC SourceOne 是一个强大的归档解决方案，用于处理来自不同协作和消息系统的电子邮件、文件和数据。 DELL Dell EMC OpenManage Server Administrator 是美国 DELL 公司的一套系统管理解决方案。该方案支持在线诊断、系统运行情况检测、设备管理等。Microsoft Windows 是美国 Microsoft 公司的一种桌面操作系统。DELL Dell EMC Avamar Server 是美国戴尔（DELL）公司的一套用于服务器的完全虚拟化的备份和恢复软件。Dell EMC PowerScale OneFS 是一款由 API 驱动的文件系统。Dell EMC PowerStore 是美国戴尔（Dell）公司的一款存储设备。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在应用程序的底层 OS 上执行任意 OS 命令，将权限提升到 root 用户，获取受影响系统的管理员访问权限。

CNVD 收录的相关漏洞包括：Dell EMC PowerScale OneFS 操作系统命令注入漏洞、Dell EMC Isilon OneFS 和 Dell EMC PowerScale OneFS 权限提升漏洞、Dell EMC SourceOne 跨站脚本漏洞、Dell EMC OpenManage Server Administrator 身份验证绕过漏洞、Dell EMC Avamar Server 授权问题漏洞、Dell EMC PowerScale OneFS 权限提升漏洞（CNVD-2021-13937、CNVD-2021-13938）、Dell EMC PowerStore 信息泄露漏洞（CNVD-2021-13943）。其中，“Dell EMC PowerScale OneFS 操作系统命令注入漏洞、Dell EMC Isilon OneFS 和 Dell EMC PowerScale OneFS 权限提升漏洞、Dell EMC SourceOne 跨站脚本漏洞”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-2021-13939

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13944

https://www.cnvd.org.cn/flaw/show/CNVD-2021-14405

https://www.cnvd.org.cn/flaw/show/CNVD-2021-14757

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13932

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13937

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13938

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13943

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。Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致本地特权升级，实现远程代码执行，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Google Android System 权限提升漏洞（CNVD-2021-13687、CNVD-2021-13691、CNVD-2021-13690）、Google Android System 远程代码执行漏洞（CNVD-2021-13692）、Google Chrome PDFium 代码执行漏洞、Google Chrome Blink 代码执行漏洞（CNVD-2021-14180）、Google Chrome 安全绕过漏洞（CNVD-2021-14179）、Google Chrome 性能 API 安全绕过漏洞。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-2021-13687

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13691

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13690

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13692

https://www.cnvd.org.cn/flaw/show/CNVD-2021-14178

https://www.cnvd.org.cn/flaw/show/CNVD-2021-14180

https://www.cnvd.org.cn/flaw/show/CNVD-2021-14179

https://www.cnvd.org.cn/flaw/show/CNVD-2021-14184

3、Adobe 产品安全漏洞

Adobe Magento 是 Adobe 公司旗下一款用 PHP 编写的开源电子商务平台。Magento Community Edition 是社区版，后改称 Magento Open Source，Magento Enterprise Edition 是企业版，后改称 Magento Commerce。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访问受限资源，执行任意代码，在浏览器中执行任意 JavaScript 等。

CNVD 收录的相关漏洞包括：Adobe Magento 用户会话无效化不足漏洞（CNVD-2021-13915、CNVD-2021-13916）、Adobe Magento 安全绕过漏洞（CNVD-2021-13928、CNVD-2021-13929）、Adobe Magento 命令注入漏洞、Adobe Magento 跨站脚本漏洞（CNVD-2021-13917）、Adobe Magento XML 注入漏洞（CNVD-2021-13921）、Adobe Magento 不当授权漏洞（CNVD-2021-13920）。其中，“Adobe Magento 用户会话无效化不足漏洞（CNVD-2021-13915、CNVD-2021-13916）、Adobe Magento 安全绕过漏洞（CNVD-2021-13928、CNVD-2021-13929）、Adobe Magento 命令注入漏洞”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-2021-13916
https://www.cnvd.org.cn/flaw/show/CNVD-2021-13915
https://www.cnvd.org.cn/flaw/show/CNVD-2021-13929
https://www.cnvd.org.cn/flaw/show/CNVD-2021-13928
https://www.cnvd.org.cn/flaw/show/CNVD-2021-13927
https://www.cnvd.org.cn/flaw/show/CNVD-2021-13917
https://www.cnvd.org.cn/flaw/show/CNVD-2021-13921
https://www.cnvd.org.cn/flaw/show/CNVD-2021-13920

4、HCL 产品安全漏洞

HCL Notes 是印度 HCL 公司的一个本地电子邮件客户端。HCL Domino 是印度 HCL 公司的一套企业级应用程序开发平台。HCL Digital Experience 是印度 HCL 公司的一套数字体验平台，内容交付解决方案。HCL iNotes 是用于访问 HCLDomino 邮件、联系人、日历、计划和协作功能的浏览客户端。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞诱使最终用户输入敏感信息，导致程序崩溃或将代码注入系统，代码将以当前登录用户的权限执行，使 Domino 崩溃或在服务器系统上执行攻击者控制的代码等。

CNVD 收录的相关漏洞包括：HCL Notes 栈缓冲区溢出漏洞、HCL Domino 缓冲区溢出漏洞、HCL Digital Experience 信息泄露漏洞、HCL iNotes 标签钓鱼漏洞、HCL Notes Email Compose 缓冲区溢出漏洞、HCL Digital Experience 访问控制错误漏洞、HCL Domino 登录跨站请求伪造漏洞、HCL Domino 安全策略绕过漏洞。其中“HCL Notes 栈缓冲区溢出漏洞、HCL Domino 缓冲区溢出漏洞”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-2021-13704
https://www.cnvd.org.cn/flaw/show/CNVD-2021-13706
https://www.cnvd.org.cn/flaw/show/CNVD-2021-13662

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13702

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13712

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13700

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13708

https://www.cnvd.org.cn/flaw/show/CNVD-2021-13707

5、Typora 跨站脚本漏洞（CNVD-2021-14407）

Typora 是一款编辑器。本周，Typora 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行远程代码。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-2021-14407

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-2021-13245	Smart 模板引擎注入漏洞（CNVD-2021-13245）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/smarty-php/smarty
CNVD-2021-13248	Apache Solr 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mail-archive.com/announce@apache.org/msg06149.html
CNVD-2021-13472	Aruba ClearPass Policy Manager 权限提升漏洞（CNVD-2021-13472）	高	目前，厂商已发布了漏洞修复程序，请及时关注更新：https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-004.txt
CNVD-2021-13676	Synology DiskStation Manager 越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.synology.com/en-global/security/advisory/Synology_SA_20_26
CNVD-2021-13476	Aruba ClearPass Policy Manager 命令注入漏洞（CNVD-2021-13476）	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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-004.txt
CNVD-2021-13675	Synology DiskStation Manager 栈缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://www.synology.com/en-global/security/advisory/Synology_SA_20_26
CNVD-2021-13964	Mofi Network MOFI4500-4GXeLTE 未授权 RCE 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：

			http://mofinetwork.com/
CNVD-2021-13965	Mofi Network MOFI4500-4GXeLTE 认证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://mofinetwork.com/
CNVD-2021-14145	ELECOM WRC-300FEBK-S 任意命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.elecom.co.jp/news/security/20210126-01/
CNVD-2021-14150	Nagios XI 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gist.github.com/leommxj/93edce6f8572cefe79a3d7da4389374e

小结：本周，DELL 产品被披露存在多个漏洞，攻击者可利用漏洞在应用程序的底层 OS 上执行任意 OS 命令，将权限提升到 root 用户，获取受影响系统的管理员访问权限。此外，Google、Adobe、HCL 等多款产品被披露存在多个漏洞，攻击者可利用漏洞未经授权访问受限资源，导致本地特权升级，实现远程代码执行，导致拒绝服务等。另外，Typora 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行远程代码。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、PHPSHE SQL 注入漏洞（CNVD-2021-14156）

验证描述

PHPSHE 是中国灵宝简好网络科技（PHPSHE）公司的一套网上商城系统。该系统支持快递跟踪、在线聊天、订单评价和数据统计等功能。

PHPSHE 中存在 SQL 注入漏洞，该漏洞源于基于数据库的应用缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令。

验证信息

POC 链接：https://gitee.com/koyshe/phpshe/issues/ITLK2

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-14156

信息提供者

北京天融信网络安全技术有限公司

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. CISA 发布关于 Microsoft Exchange 漏洞在野利用的紧急指令

在 Microsoft 发布带外补丁程序以解决 Microsoft Exchange Server 本地版本中的多个零日漏洞之后，美国网络安全和基础结构安全局（CISA）发出了紧急指示警告，称攻击者“主动利用”漏洞。

参考链接：https://thehackernews.com/2021/03/cisa-issues-emergency-directive-on-in.html

2. 新的 Chrome 0day 漏洞正被利用

Google 本周发布了 Chrome 的安全更新 v89.0.4389.72，修复了 47 个漏洞，其中包括正被利用 0day。编号为 CVE-2021-21166 的漏洞是微软安全研究员 Alison Huffman 在 2 月 11 日报告的，Google 没有披露漏洞细节，只是表示它知道漏洞正被利用。

参考链接：https://www.solidot.org/story?sid=67100

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