国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 12 月 28 日-2021 年 01 月 03 日　　2020 年第 53 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 295，其中高危漏洞 116 个、中危漏洞 152 个、低危漏洞 27 个。漏洞平均分值为 5.92。本周收录的漏洞中，涉及 0day 漏洞 174 个（占 59%），其中互联网上出现“OpenCart 跨站脚本漏洞（CNVD-2020-75516）、IncomCMS 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 6932 个，与上周（11489 个）环比减少 40%。

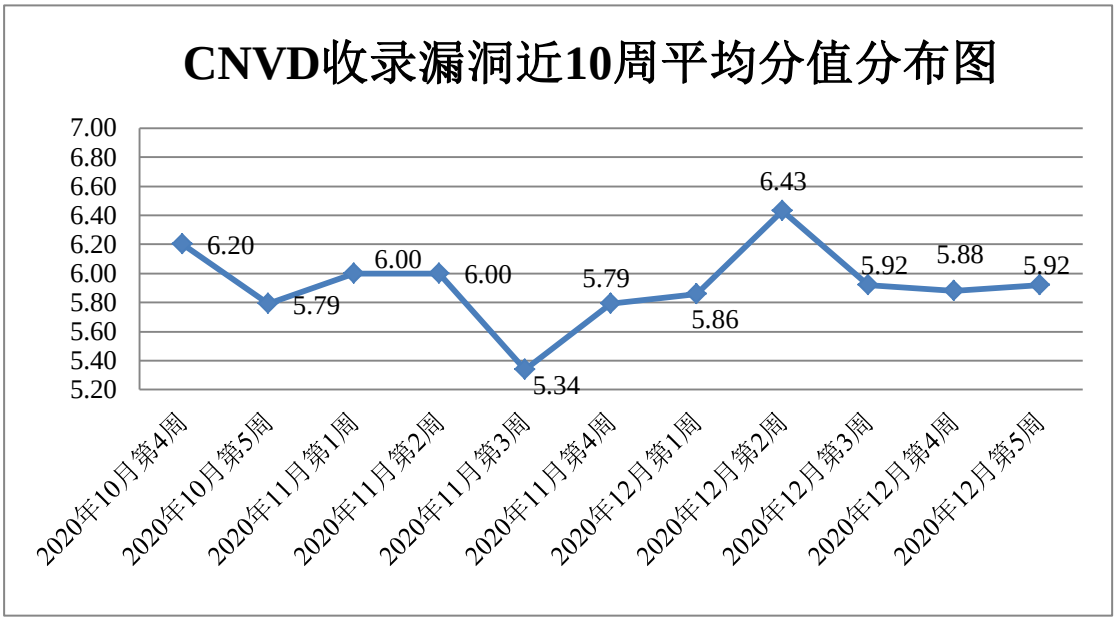

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 18 起，向基础电信企业通报漏洞事件 7 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 269 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 66 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 21 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：

飞狐信息技术（天津）有限公司、北京爱奇艺科技有限公司、北京风行在线技术有限公司、云南华企优享网络科技有限公司、深圳市网旭科技有限公司、湖南星云网络信息技术有限公司、广州虎牙信息科技有限公司、深圳市富途网络科技有限公司、中电鸿信信息科技有限公司、淄博闪灵网络科技有限公司、湖南壹拾捌号网络技术有限公司、深圳市创想天空科技股份有限公司、北京猎鹰安全科技有限公司、上海泛微网络科技股份有限公司、金山软件股份有限公司、郑州微口网络科技有限公司、重庆逐越光电科技有限公司、浙江大华技术股份有限公司、北京百度网讯科技有限公司、广州网易计算机系统有限公司、广州津虹网络传媒有限公司、小咖秀（北京）科技有限公司、上海宽娱数码科技有限公司、北京海腾时代科技有限公司、河南青峰网络科技有限公司、微点佰慧（北京）信息安全技术有限公司、上海聚力传媒技术有限公司、南京传唱软件科技有限公司、桂林市亿星网络科技有限责任公司、上海泛微网络科技有限公司、上海畅指网络科技有限公司、深圳坐标软件集团有限公司、珠海金山办公软件有限公司、明镜远大网络安全信息技术有限公司、西门子（中国）有限公司、杭州网易质云科技有限公司、北京坤豆科技有限公司、桂林崇胜网络科技有限公司、西安交大捷普网络科技有限公司、深圳维盟科技股份有限公司、深圳市爱思软件技术有限公司、广州国微软件科技有限公司、北京搜狗信息服务有限公司、湖南一唯信息科技有限公司、济南点量软件有限公司、科大讯飞股份有限公司、北京火绒网络科技有限公司、北京多点在线科技有限公司、华林证券股份有限公司、北京江民新科技术有限公司、南昌维网数字传媒有限公司、上海二三四五移动科技有限公司、博韩伟业（北京）科技有限公司、台达电子企业管理(上海)有限公司、上海亿速网络科技有限公司、杭州凯凯科技有限公司、北京聪明核桃教育科技有限公司、郑州木云电子科技有限公司、广州合优网络科技有限公司、锐捷网络股份有限公司、趋势科技和 HEYBBS。

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、北京神州绿盟科技有限公司、厦门服云信息科技有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。北京山石网科信息技术有限公司、国瑞数码零点实验室、北京华云安信息技术有限公司、南京众智维信息科技有限公司、江苏保旺达软件技术有限公司、北京天地和兴科技有限公司、山东华鲁科技发展股份有限公司、山东新潮信息技术有限公司、河南灵创电子科技有限公司、河南信安世纪科技

有限公司、北京赛克艾威科技有限公司、西安交大捷普网络科技有限公司、浙江安腾信息技术有限公司、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、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、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）、内蒙古奥创科技有限公司、重庆都会信息科技有限公司、广州市蓝爵计算机科技有限公司、北京机沃科技有限公司、浙江大学 307LAB、山石网科通信技术股份有限公司、安徽长泰信息安全服务有限公司、北京智游网安科技有限公司、山东正中信息技术股份有限公司、腾讯安全天马实验室、新疆海狼科技有限公司、武汉明嘉信信息安全检测评估有限公司、长扬科技（北京）有限公司、北京明朝万达科技股份有限公司（安元实验室）、北京惠而特科技有限公司、四川哨兵信息科技有限公司及其他个人白帽子向 CNVD 提交了 6932 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 5446 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）	4360	4360
斗象科技（漏洞盒子）	597	597
上海交大	489	489
北京天融信网络安全技术有限公司	246	2
哈尔滨安天科技集团股份有限公司	219	0
北京神州绿盟科技有限公司	176	10
厦门服云信息科技有限公司	123	0
华为技术有限公司	86	0
新华三技术有限公司	75	0
深信服科技股份有限公司	61	0
北京启明星辰信息安全技术有限公司	53	0
北京数字观星科技有限公司	50	0
中国电信股份有限公司网络安全产品运营中心	20	0
中国电信集团系统集成有限责任公司	17	17
沈阳东软系统集成工程有限公司	7	7
北京知道创宇信息技术股份有限公司	1	0
北京山石网科信息技术有限公司	212	212
国瑞数码零点实验室	104	104

北京华云安信息技术有限公司	103	103
北京华顺信安科技有限公司	100	0
南京众智维信息科技有限公司	64	64
江苏保旺达软件技术有限公司	51	51
北京天地和兴科技有限公司	47	47
山东华鲁科技发展股份有限公司	36	36
山东新潮信息技术有限公司	33	33
河南灵创电子科技有限公司	32	32
河南信安世纪科技有限公司	32	32
北京赛克艾威科技有限公司	19	19
西安交大捷普网络科技有限公司	18	18
浙江安腾信息技术有限公司	17	17
杭州迪普科技股份有限公司	14	0
上海犀点意象网络科技有限公司	11	11
山东云天安全技术有限公司	11	11
杭州海康威视数字技术股份有限公司	11	11
上海观安信息技术股份有限公司	9	9
远江盛邦（北京）网络安全科技股份有限公司	8	8
北京云科安信科技有限公司（Seraph 安全实验室）	8	8
内蒙古奥创科技有限公司	5	5
重庆都会信息科技有限公司	4	4
广州市蓝爵计算机科技有限公司	4	4
北京机沃科技有限公司	2	2
浙江大学 307LAB	2	2
山石网科通信技术股份有限公司	2	2
安徽长泰信息安全服务有限公司	2	2
北京智游网安科技有限公司	1	1
山东正中信息技术股份有限公司	1	1
腾讯安全天马实验室	1	1

新疆海狼科技有限公司	1	1
武汉明嘉信信息安全检测评估有限公司	1	1
长扬科技（北京）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
北京惠而特科技有限公司	1	1
四川哨兵信息科技有限公司	1	1
CNCERT 浙江分中心	7	7
CNCERT 新疆分中心	1	1
CNCERT 西藏分中心	1	1
CNCERT 山东分中心	1	1
个人	584	584
报送总计	8144	6932

本周漏洞按类型和厂商统计

本周，CNVD 收录了 295 个漏洞。应用程序 131 个，WEB 应用 105 个，操作系统 28 个，网络设备（交换机、路由器等网络端设备）23 个，智能设备（物联网终端设备）5 个，安全产品 3 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	131
WEB 应用	105
操作系统	28
网络设备（交换机、路由器等网络端设备）	23
智能设备（物联网终端设备）	5
安全产品	3

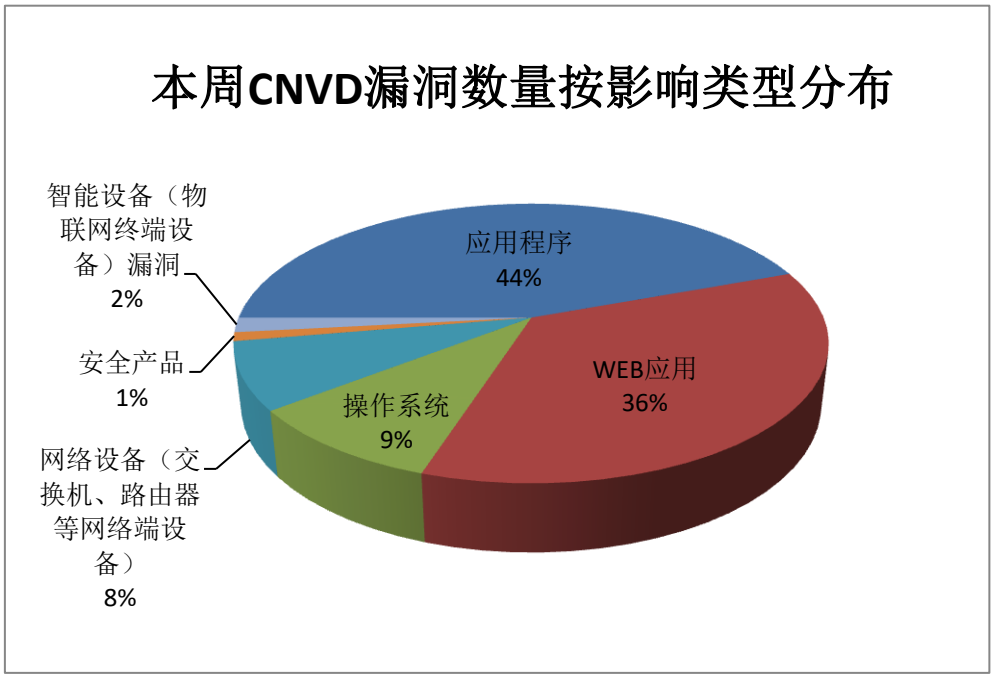

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Dell、SAP 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	26	9%
2	Dell	16	5%
3	SAP	11	4%
4	F5	10	4%
5	Zammad	9	3%
6	IBM	8	3%
7	NETGEAR	8	3%
8	华安证券股份有限公司	7	2%
9	HPE	7	2%
10	其他	193	65%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，24 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“NETGEAR DGN2200v1 命令注入漏洞”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/

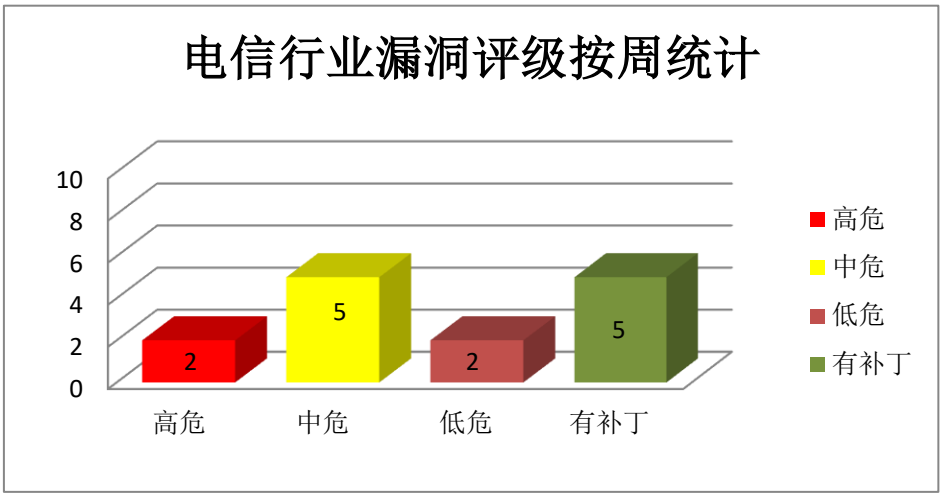

图 3 电信行业漏洞统计

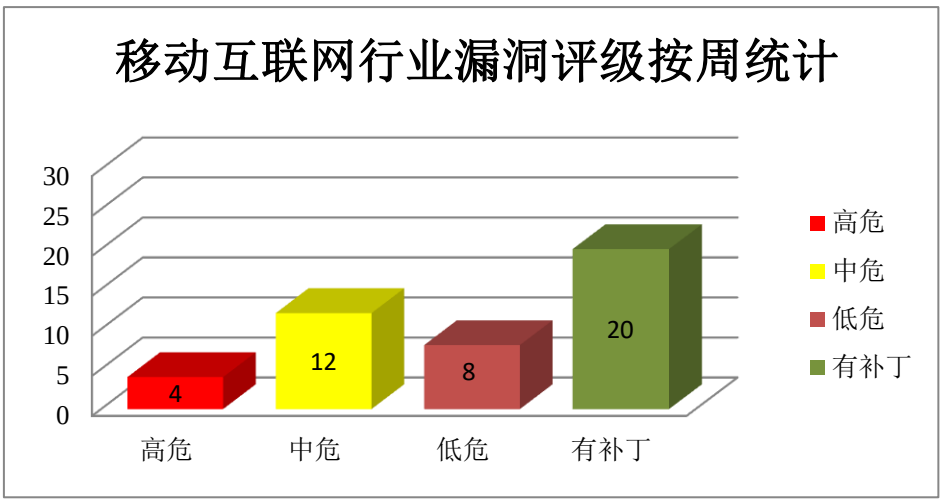

图 4 移动互联网行业漏洞统计

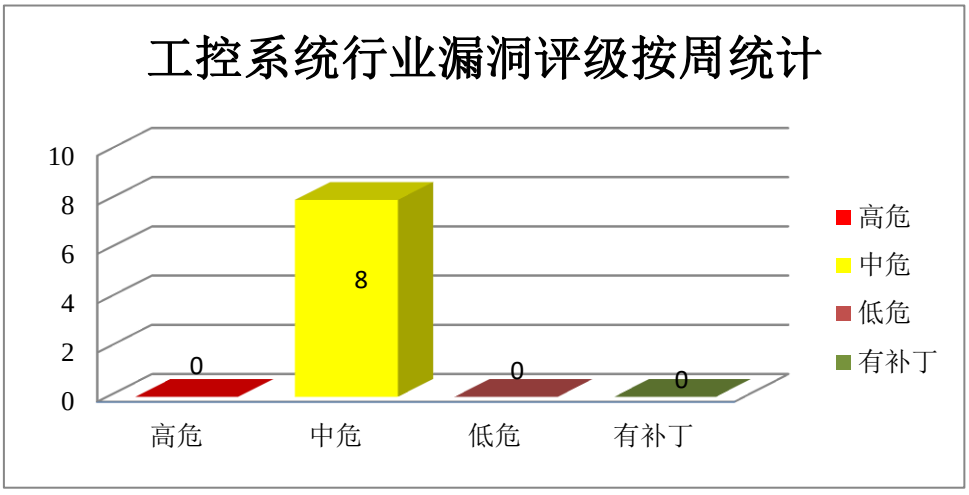

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Google Android 是美国谷歌（Google）和开放手持设备联盟（简称 oha）的一套以 Linux 为基础的开源操作系统。Google TensorFlow 是一套用于机器学习的端到端开源平台。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，导致应用崩溃等。

CNVD 收录的相关漏洞包括：Google Android 资源管理错误漏洞（CNVD-2020-75039、CNVD-2020-75040）、Google Android 缓冲区溢出漏洞（CNVD-2020-75048、CNVD-2020-75052）、Google Android 信息泄露漏洞（CNVD-2020-75051）、Google Android 权限提升漏洞（CNVD-2020-75053）、Google TensorFlow 缓冲区溢出漏洞（CNVD-2021-00089、CNVD-2021-00091）。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-2020-75039

https://www.cnvd.org.cn/flaw/show/CNVD-2020-75040

https://www.cnvd.org.cn/flaw/show/CNVD-2020-75048

https://www.cnvd.org.cn/flaw/show/CNVD-2020-75052

https://www.cnvd.org.cn/flaw/show/CNVD-2020-75051

https://www.cnvd.org.cn/flaw/show/CNVD-2020-75053

https://www.cnvd.org.cn/flaw/show/CNVD-2021-00089

https://www.cnvd.org.cn/flaw/show/CNVD-2021-00091

2、Dell 产品安全漏洞

Dell EMC Unisphere for PowerMax 是一套针对 PowerMax 存储阵列的图形化管理工具。Dell Dell EMC iDRAC9 是一套包含硬件和软件的系统管理解决方案。Dell BSAFE Micro Edition Suite 是一个可为 c/c++应用、设备、系统提供加密、证书和传输层安全性的开发工具包。Dell EMC NetWorker 是一套统一备份和恢复软件。Dell EMC Isilon OneFS 和 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 PowerProtect Data Manager 是一套数据保护解决方案。PowerProtect X400 是一款数据管理设备。Dell Encryption 是一套数据保护解决方案。Dell Endpoint Security Suite 是一套网络安全套件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，访问未经授权的文件，在网站的上下文中运行 JavaScript 代码等。

CNVD 收录的相关漏洞包括：Dell EMC Unisphere for PowerMax 跨站脚本漏洞、DELL Dell EMC iDRAC9 跨站脚本漏洞、Dell BSAFE Micro Edition Suite 缓冲区溢出漏洞、Dell EMC NetWorker 不当授权漏洞、Dell EMC Isilon OneFS 和 EMC PowerScale OneFS 权限提升漏洞、Dell EMC Isilon OneFS 和 EMC PowerScale 文件权限漏洞、Dell PowerProtect Data Manager 和 PowerProtect X400 授权问题漏洞、Dell Encryption

和 Dell Endpoint Security Suite 权限提升漏洞。其中，“Dell Encryption 和 Dell Endpoint Security Suite 权限提升漏洞”的综合评级为“中危”。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-2021-00014
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00022
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00021
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00030
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00035
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00040
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00038
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00037

3、SAP 产品安全漏洞

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 3D Visual Enterprise Viewer 是一款应用软件。SAP Business Warehouse（BW）是 SAP 的数据仓库解决方案。SAP Disclosure Management 是一套自动化财务披露管理系统。SAP Identity Management 是一套能够嵌入到业务流程中的身份管理应用程序。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。SAP Netweaver 是一套面向服务的集成化应用平台。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或劫持用户会话，在应用程序中执行注入的文件或代码，导致目标主机应用程序崩溃等。

CNVD 收录的相关漏洞包括：SAP Solution Manager 开放重定向漏洞、SAP 3D Visual Enterprise Viewer 输入验证错误漏洞（CNVD-2020-74930、CNVD-2020-74931）、SAP Business Warehouse 和 SAP BW4HANA 操作系统命令注入漏洞、SAP Disclosure Management 代码问题漏洞（CNVD-2020-74927）、SAP Identity Management 信息泄露漏洞（CNVD-2020-74932）、SAP Business Objects Business Intelligence Platform 注入漏洞、SAP NetWeaver AS ABAP 跨站脚本漏洞。其中，“SAP Business Warehouse 和 SAP BW4HANA 操作系统命令注入漏洞”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-2020-74925
https://www.cnvd.org.cn/flaw/show/CNVD-2020-74930
https://www.cnvd.org.cn/flaw/show/CNVD-2020-74928
https://www.cnvd.org.cn/flaw/show/CNVD-2020-74927
https://www.cnvd.org.cn/flaw/show/CNVD-2020-74932
https://www.cnvd.org.cn/flaw/show/CNVD-2020-74931

https://www.cnvd.org.cn/flaw/show/CNVD-2020-74933

https://www.cnvd.org.cn/flaw/show/CNVD-2021-00095

4、F5 产品安全漏洞

F5 BIG-IP 是一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。F5 BIG-IP ASM 是一款 Web 应用程序防火墙（WAF），它提供安全的远程接入、保护电子邮件、简化 Web 接入控制，同时增强网络和应用性能。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，在网站的上下文中运行 JavaScript 代码，触发拒绝服务等。

CNVD 收录的相关漏洞包括：F5 BIG-IP ASM 拒绝服务漏洞（CNVD-2020-74859、CNVD-2020-74866）、F5 BIG-IP 拒绝服务漏洞（CNVD-2020-74858、CNVD-2020-74870）、F5 BIG-IP 跨站脚本漏洞（CNVD-2020-74864）、F5 BIG-IP 信息泄露漏洞（CNVD-2020-74865）、F5 BIG-IP 安全绕过漏洞、F5 BIG-IP VE 资源管理错误漏洞。其中，“F5 BIG-IP 拒绝服务漏洞（CNVD-2020-74858）、F5 BIG-IP 拒绝服务漏洞（CNVD-2020-74870）”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-2020-74859

https://www.cnvd.org.cn/flaw/show/CNVD-2020-74858

https://www.cnvd.org.cn/flaw/show/CNVD-2020-74864

https://www.cnvd.org.cn/flaw/show/CNVD-2020-74866

https://www.cnvd.org.cn/flaw/show/CNVD-2020-74865

https://www.cnvd.org.cn/flaw/show/CNVD-2020-74871

https://www.cnvd.org.cn/flaw/show/CNVD-2020-74870

https://www.cnvd.org.cn/flaw/show/CNVD-2020-74869

5、phpList SQL 注入漏洞（CNVD-2020-75154）

phpList 是英国 phpList 公司的一套开源的新闻通讯和电子邮件营销软件。本周，phpList 被披露存在 SQL 注入漏洞。攻击者可通过"Config - Import Administrators"页面的第 4 行属性利用该漏洞注入 SQL 查询。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-2020-75154

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-2020-74852	Belkin LINKSYS RE6500 远程代码执行漏洞	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：

			https://www.linksys.com/us/support-article?articleNum=148460
CNVD-2020-74863	Foxit Reader 越界写漏洞	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.foxitsoftware.com/support/security-bulletins.html
CNVD-2020-74862	Mozilla Firefox WebGL 堆缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.mozilla.org/en-US/security/advisories/mfsa2020-54/
CNVD-2020-75058	Zammad SSO 端点认证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://zammad.com/en/advisories/zaa-2020-18
CNVD-2020-75064	HCL Domino 拒绝服务漏洞（CNVD-2020-75064）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0085947&sys_kb_id=bbf4eb6a1bd52490534c4159cc4bcb04
CNVD-2020-75517	NETGEAR DGN2200v1 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kb.netgear.com/000062634/Security-Advisory-for-Command-Injection-Vulnerability-on-DGN2200v1-PSV-2020-0411
CNVD-2021-00015	HPE iLO Amplifier Pack server 远程代码执行漏洞	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-hpesbgn04067en_us
CNVD-2021-00023	Apple macOS 缓冲区溢出漏洞（CNVD-2021-00023）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/zh-cn/HT211931
CNVD-2021-00025	HPE Edgeline Infrastructure Management 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://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04063en_us
CNVD-2021-00019	Apple macOS 内存破坏漏洞（CNVD-2021-00019）	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/en-us/HT212005

小结：本周，Google 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，导致应用崩溃等。此外，Dell、SAP、F5 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，访问未经授权的文件，获取敏感信息或劫持用户会话，在网站的上下文中运行 JavaScript 代码，触发拒绝服务等。另外，phpList 被披露存在 SQL 注入漏洞。攻击者可通过"Config - Import Administrators"页面的第 4 行属性利用该漏洞注入 SQL 查询。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、OpenCart 跨站脚本漏洞（CNVD-2020-75516）

验证描述

OpenCart 是一个基于 PHP 的开源在线电子商务解决方案。

OpenCart 3.0.3.6 中的 Profile Image 存在跨站脚本漏洞。攻击者可利用该漏洞上传并执行恶意代码。

验证信息

POC 链接：https://www.exploit-db.com/exploits/49098

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-75516

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. Google 文档漏洞可能允许黑客查看私人文档

谷歌已经修补了其服务中集成的反馈工具中的一个漏洞，攻击者可以利用该漏洞嵌入恶意代码，从而窃取敏感的 Google Docs 文档的屏幕快照。

参考链接：https://thehackernews.com/2020/12/a-google-docs-bug-could-have-allowed.html

2. 微软即将推出 Windows 10 随机清除已保存登录凭证的 Bug 补丁

今年 11 月，微软证实 Windows 10 存在一个可能导致系统无法记住 Chrome、Edge、OneDrive 等软件密码的 Bug。然而由于问题的随机性，导致开发团队难以追溯其根源。受影响的用户，也只能一遍遍地重复输入相关的登录凭证（用户名和密码）。

参考链接：https://www.cnbeta.com/articles/tech/1071561.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