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 14 日-2020 年 12 月 20 日　　2020 年第 51 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 214 个，其中高危漏洞 80 个、中危漏洞 125 个、低危漏洞 9 个。漏洞平均分值为 5.92。本周收录的漏洞中，涉及 0day 漏洞 143 个（占 67%），其中互联网上出现“Online Bus Ticket Reservation SQL 注入漏洞、BloodX 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 12185 个，与上周（12235 个）环比减少 0.4%。

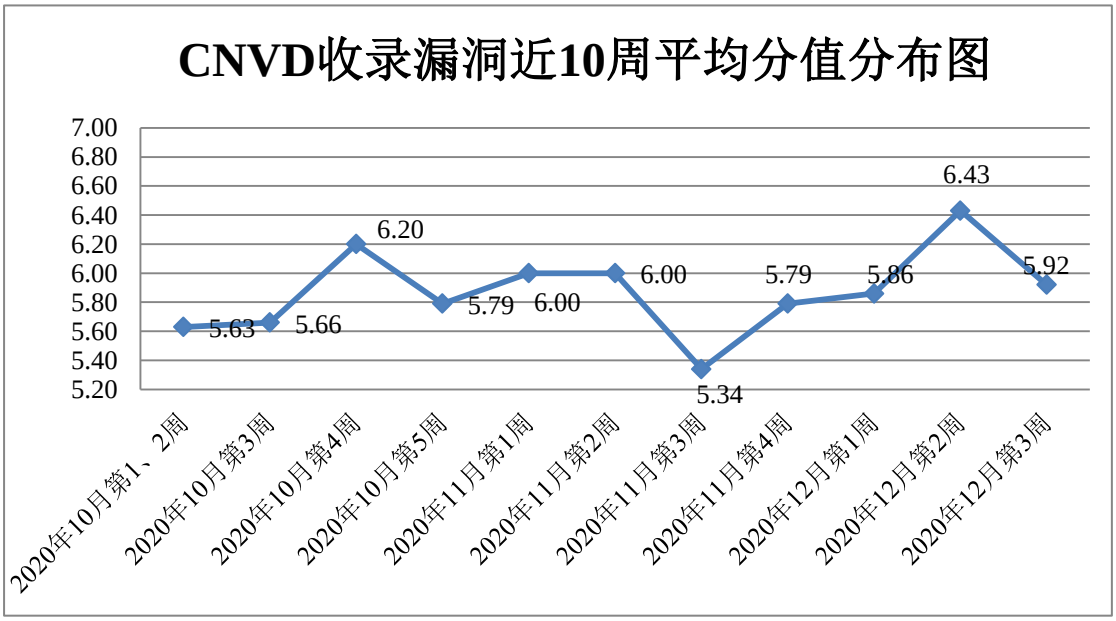

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 30 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 329 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 21 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 43 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：

网际傲游(北京)科技有限公司、小船出海教育科技（北京）有限公司、北京数码大方科技股份有限公司、上海二三四五移动科技有限公司、上海广乐网络科技有限公司、北京因酷时代科技有限公司、广东睿江云计算股份有限公司、深圳市星空量子科技有限公司、上海百胜软件股份有限公司、北京易普拉格科技股份有限公司、浙江快服集团有限公司、北京通达信科科技有限公司、长沙米拓信息技术有限公司、ACS 运动控制中国（上海）、工业供热与制冷有限公司、郑州天迈科技股份有限公司、青岛商至信网络科技有限公司、杭州新中大科技股份有限公司、网易有道信息技术（北京）有限公司、苏州思杰马克丁软件有限公司、金蝶软件（中国）有限公司、郑州微口网络科技有限公司、上海泛微网络科技股份有限公司、北京尚网汇智科技有限公司、江苏三希科技股份有限公司、上海迈微软件科技有限公司、方法数码（成都）科技有限公司、北京百度网讯科技有限公司、黄山生活在线信息科技有限公司、广州网易计算机系统有限公司、江苏连邦信息技术有限公司、北京威速科技有限公司、成都俊云科技有限公司、普联技术有限公司、北京多点在线科技有限公司、淄博闪灵网络科技有限公司、锐捷网络股份有限公司、瑞芯微电子股份有限公司、青岛软媒网络科技有限公司、北京搜狗信息服务有限公司、广州齐博网络科技有限公司、厦门网中网软件有限公司、浙江中控技术股份有限公司、上海牛迈网络科技有限公司、福建福昕软件开发股份有限公司、深圳市盛世桃源网络科技有限公司、成都市任我行信息技术有限公司、上海阿法迪智能标签系统技术有限公司、深圳市信锐网科技术有限公司、联想集团、上海荃路软件开发工作室、米酷影视、佳佳软件、VMware、Eltima、SEACMS、FUEL CMS、YzmCMS 、UCMS 、LzCMS 、CIMCO 和 SEMCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、北京天融信网络安全技术有限公司、厦门服云信息科技有限公司、阿里云计算有限公司、哈尔滨安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。国瑞数码零点实验室、北京山石网科信息技术有限公司、山东华鲁科技发展股份有限公司、北京天地和兴科技有限公司、河南灵创电子科技有限公司、山东云天安全技术有限公司、新疆海狼科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、远江盛邦（北京）网络安全科技股份有限公司、河南信安世纪科技有限公司、南京众智维信息科技有限公司、浙江安腾信息技术有限公司、北京机沃科技有限公司、广州市蓝爵计算机科技有限公司、内蒙古奥

创科技有限公司、上海观安信息技术股份有限公司、山东道普测评技术有限公司、郑州云智信安安全技术有限公司、安徽长泰信息安全服务有限公司、北京长亭科技有限公司、吉林谛听信息技术有限公司、广州万方计算机科技有限公司、长扬科技（北京）有限公司、广州百蕴启辰科技有限公司、北京智游网安科技有限公司、北京时代新威信息技术有限公司、深圳市魔方安全科技有限公司、上海纽盾科技股份有限公司及其他个人白帽子向 CNVD 提交了 12185 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 10376 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）	5855	5855
斗象科技（漏洞盒子）	3838	3838
上海交大	683	683
北京神州绿盟科技有限公司	433	0
北京天融信网络安全技术有限公司	431	1
厦门服云信息科技有限公司	340	0
阿里云计算有限公司	283	0
哈尔滨安天科技集团股份有限公司	254	0
华为技术有限公司	117	0
新华三技术有限公司	105	0
深信服科技股份有限公司	80	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
中国电信集团系统集成有限责任公司	46	46
中国电信股份有限公司网络安全产品运营中心	20	0
北京知道创宇信息技术股份有限公司	5	0
沈阳东软系统集成工程有限公司	3	3
国瑞数码零点实验室	193	193
北京山石网科信息技术有限公司	97	97
山东华鲁科技发展股份有限公司	32	32
北京天地和兴科技有限公司	28	28
河南灵创电子科技有限公司	26	26

山东云天安全技术有限公司	21	21
新疆海狼科技有限公司	20	20
北京云科安信科技有限公司（Seraph 安全实验室）	18	18
杭州迪普科技股份有限公司	15	0
远江盛邦（北京）网络安全科技股份有限公司	15	15
河南信安世纪科技有限公司	14	14
南京众智维信息科技有限公司	14	14
浙江安腾信息技术有限公司	13	13
北京机沃科技有限公司	8	8
广州市蓝爵计算机科技有限公司	8	8
内蒙古奥创科技有限公司	7	7
上海观安信息技术股份有限公司	6	6
山东道普测评技术有限公司	5	5
郑州云智信安安全技术有限公司	3	3
安徽长泰信息安全服务有限公司	3	3
北京长亭科技有限公司	2	2
吉林谛听信息技术有限公司	1	1
广州万方计算机科技有限公司	1	1
长扬科技（北京）有限公司	1	1
广州百蕴启辰科技有限公司	1	1
北京智游网安科技有限公司	1	1
北京时代新威信息技术有限公司	1	1
深圳市魔方安全科技有限公司	1	1
上海纽盾科技股份有限公司	1	1
CNCERT 山东分中心	2	2
CNCERT 贵州分中心	2	2
CNCERT 四川分中心	1	1
个人	1213	1213
报送总计	14370	12185

本周漏洞按类型和厂商统计

本周，CNVD 收录了 214 个漏洞。应用程序 120 个，WEB 应用 71 个，操作系统 1

4 个，网络设备（交换机、路由器等网络端设备）5 个，数据库 3 个，安全产品 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	120
WEB 应用	71
操作系统	14
网络设备（交换机、路由器等网络端设备）	5
数据库	3
安全产品	1

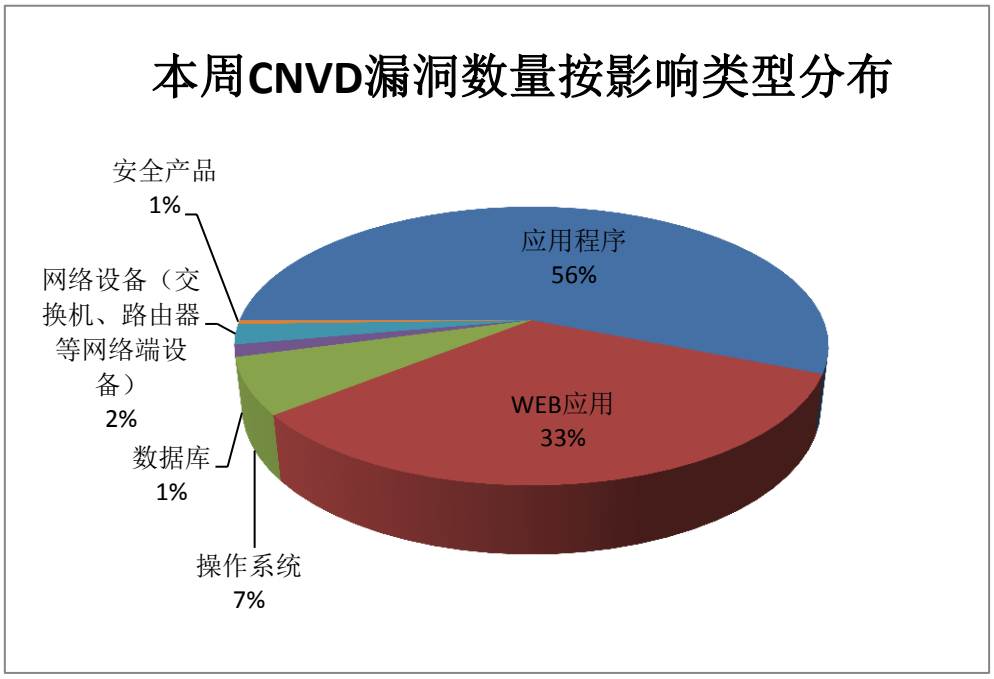

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 JerryScript、Microsoft、Oracle 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	JerryScript	45	21%
2	Microsoft	14	7%
3	Oracle	13	6%
4	Mozilla	8	4%
5	Cisco	8	4%
6	Google	8	4%
7	Pixar	7	3%
8	上海荃路软件开发工作室	5	2%

9	Moddable	5	2%
10	其他	101	47%

本周行业漏洞收录情况

本周，CNVD 收录了 4 个电信行业漏洞，11 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“D-Link DSR-250 命令注入漏洞、FactoryTalk Linx 堆缓冲区溢出漏洞、Google Android System 权限提升漏洞（CNVD-2020-72495）”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/

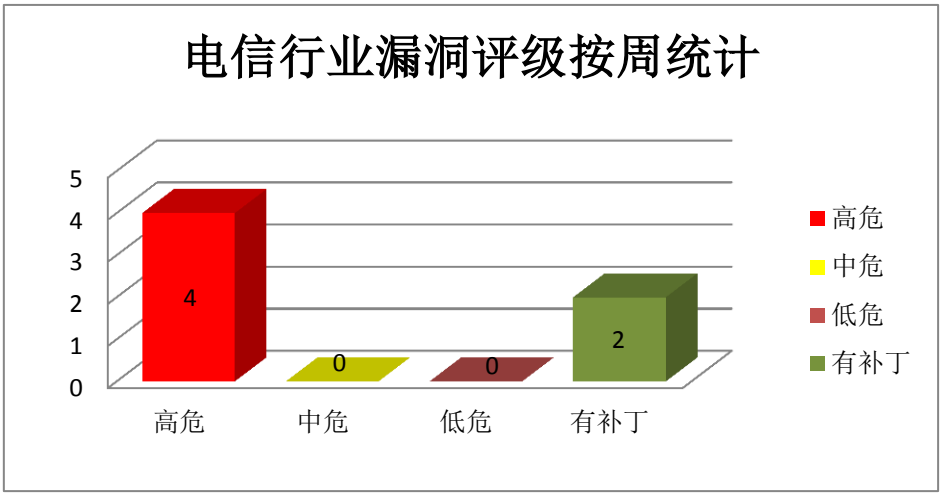

图 3 电信行业漏洞统计

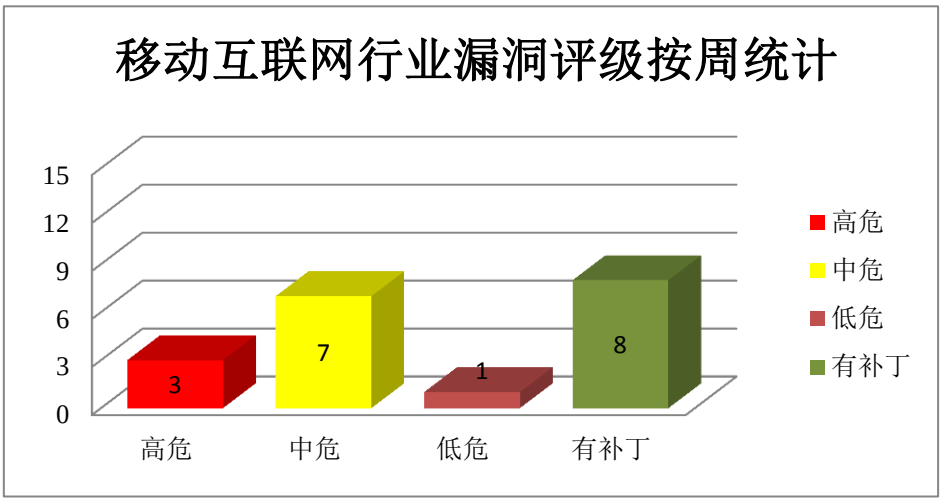

图 4 移动互联网行业漏洞统计

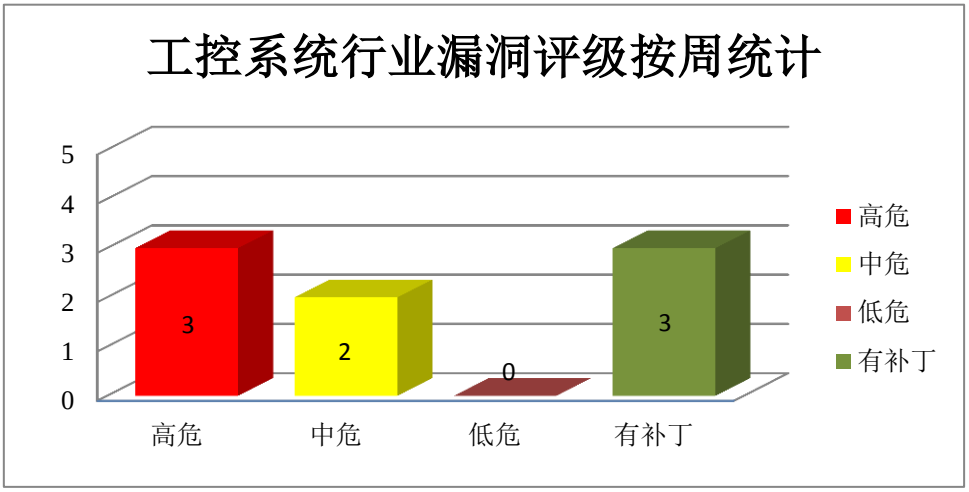

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

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。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本地权限获取敏感信息，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Google Android 信息泄露漏洞（CNVD-2020-72490）、Google Android 权限提升漏洞（CNVD-2020-72489、CNVD-2020-72491、CNVD-2020-72494）、Google Android Media Framework 信息泄露漏洞（CNVD-2020-72488）、Google Android 拒绝服务漏洞（CNVD-2020-72493、CNVD-2020-72492）、Google Android System 权限提升漏洞（CNVD-2020-72495）。其中，“Google Android 拒绝服务漏洞（CNVD-2020-72493）、Google Android System 权限提升漏洞（CNVD-2020-72495）”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-2020-72490

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72489

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72488

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72493

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72492

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72491

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72495

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72494

2、Microsoft 产品安全漏洞

Microsoft Outlook 是美国微软（Microsoft）公司的一套电子邮件应用程序。Microsoft ChakraCore 和 Microsoft Edge 都是美国微软（Microsoft）公司的产品。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 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 Codecs Library 是其中的一个音频、视频文件编解码器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统用户的上下文中运行任意代码，破坏内存，控制受影响的系统等。

CNVD 收录的相关漏洞包括：Microsoft Outlook 远程代码执行漏洞（CNVD-2020-72694）、Microsoft ChakraCore 和 Edge 远程代码执行漏洞（CNVD-2020-72698）、Microsoft Color Management 远程代码执行漏洞、Microsoft ChakraCore 远程代码执行漏洞（CNVD-2020-72699、CNVD-2020-72701、CNVD-2020-72700）、Microsoft Windows Codecs Library 远程代码执行漏洞（CNVD-2020-72695、CNVD-2020-72696）。其中，“Microsoft Outlook 远程代码执行漏洞（CNVD-2020-72694）、Microsoft ChakraCore 和 Edge 远程代码执行漏洞（CNVD-2020-72698）、Microsoft Color Management 远程代码执行漏洞、Microsoft ChakraCore 远程代码执行漏洞（CNVD-2020-72699、CNVD-2020-72701、CNVD-2020-72700）”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-2020-72694
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72698
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72697
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72699
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72701
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72700
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72695
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72696

3、Cisco 产品安全漏洞

Cisco IoT Field Network Director（IoT-FND）是美国思科（Cisco）公司的一套端到端的物联网管理系统。Cisco RoomOS Software 是美国思科（Cisco）公司的一套用于 Cisco 设备的自动管理软件。该软件主要用于升级、管理 Cisco 设备的主板固件。Cisco Security Manager（CSM）是美国思科（Cisco）公司的一套企业级的管理应用，它主要用于在 Cisco 网络和安全设备上配置防火墙、VPN 和入侵保护安全服务。Cisco IOS XE 是美国 Cisco 公司为其网络设备开发的一套基于 Linux 内核的模块化操作系统。Cisco FXOS Software 是美国思科（Cisco）公司的一套运行在思科安全设备中的防火墙软件。Cisco IoT

Field Network Director (FND)是大规模 FAN 部署的网络管理系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞查看受影响系统上的敏感信息，使用生成的令牌在设备上启用用户不应该使用的实验特性，发送特制 API 请求利用该漏洞覆盖受影响系统上的文件等。

CNVD 收录的相关漏洞包括：Cisco IoT Field Network Director 访问控制错误漏洞（CNVD-2020-72728）、Cisco RoomOS Software 权限许可和访问控制问题漏洞、Cisco Security Manager 输入验证错误漏洞（CNVD-2020-72726）、Cisco IOS XE 拒绝服务漏洞（CNVD-2020-72733）、Cisco FXOS 安全启动绕过漏洞、Cisco IoT Field Network Director 访问控制错误漏洞、Cisco IoT Field Network Director 文件覆盖漏洞、Cisco IoT Field Network Director SQL 注入漏洞。其中，“Cisco FXOS 安全启动绕过漏洞、Cisco IoT Field Network Director SQL 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-2020-72728
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72727
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72726
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72733
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72732
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72731
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72730
https://www.cnvd.org.cn/flaw/show/CNVD-2020-72729

4、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。Mozilla Thunderbird 是美国 Mozilla 基金会的一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。NSS 是美国 Mozilla 基金会的一个底层密码学库。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内存破坏和程序崩溃，导致浏览器挂起，获取 Thunderbird 的用户名和密码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 内存破坏漏洞（CNVD-2020-72461、CNVD-2020-72462、CNVD-2020-72720）、Mozilla Firefox 拒绝服务漏洞（CNVD-2020-72463）、Mozilla Firefox 欺骗漏洞（CNVD-2020-72716）、Mozilla Thunderbird 信息泄露漏洞（CNVD-2020-72718）、Mozilla NSS 拒绝服务漏洞、Mozilla Firefox 内存错误引用漏洞（CNVD-2020-72719），其中，“Mozilla Firefox 内存破坏漏洞（CNVD-2020-72461、CNVD-2020-72462）”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-2020-72461

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72462

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72463

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72716

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72718

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72717

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72720

https://www.cnvd.org.cn/flaw/show/CNVD-2020-72719

5、OpenTSDB 命令注入漏洞

OpenTSDB 是一个基于 Hbase 的分布式、可扩展的时间序列数据库(TSDB)。OpenTSDB 2.4.0 及更早版本存在命令执行漏洞。攻击者可通过 yrange 参数注入命令利用该漏洞实现远程代码执行。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-2020-72736

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-2020-71193	Moddable SDK 堆缓冲区溢出漏洞（CNVD-2020-71193）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://github.com/Moddable-OpenSource/moddable/releases/tag/OS200903
CNVD-2020-71204	Western Digital My Cloud OS 5 认证绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115
CNVD-2020-71208	FactoryTalk Linx 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://us-cert.cisa.gov/ics/advisories/icsa-20-329-01
CNVD-2020-71206	Western Digital My Cloud OS 5 NAS Admin 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://www.westerndigital.com/support/productsecurity/wdc-20009-os5-firmware-5-06-115
CNVD-2020-71205	Western Digital My Cloud OS 5 NAS Admin 认证绕过漏洞（CNVD-2020-71205）	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.westerndigital.com/support/productsecurity/wdc-20009-os5-firmwa

			re-5-06-115
CNVD-2020-71209	FactoryTalk Linx 不当输入验证漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://us-cert.cisa.gov/ics/advisories/icsa-20-329-01
CNVD-2020-72723	D-Link DSR-250 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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10195
CNVD-2020-72722	D-Link DSR-250 命令注入漏洞（CNVD-2020-72722）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10195
CNVD-2020-72732	Cisco FXOS 安全启动绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-sbbp-XTuPkYTn
CNVD-2020-72735	Kepware Linkmaster 权限许可和访问控制问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.kepware.com/en-us/products/linkmaster/

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞提升本地权限获取敏感信息，造成拒绝服务等。此外，Microsoft、Cisco、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在系统用户的上下文中运行任意代码，破坏内存，控制受影响的系统等。另外，OpenTSDB 被披露存在命令注入漏洞。攻击者可利用漏洞实现远程代码执行。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、Online Bus Ticket Reservation SQL 注入漏洞

验证描述

Sourcecodester Online Bus Ticket Reservation 是美国 Sourcecodester 公司的一个在线公交车售票平台。

Online Bus Ticket Reservation 1.0 版本存在 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任意 SQL 命令，并通过用户名和密码字段绕过身份验证。

验证信息

POC 链接：https://www.exploit-db.com/exploits/49212

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-72738

信息提供者

新华三技术有限公司

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. HPE 在 Systems Insight Manager 中披露了关键的零时差

惠普（HPE）披露了一个零日远程代码执行漏洞，该漏洞会影响其适用于 Windows 和 Linux 的 HPE Systems Insight Manager（SIM）软件的最新版本。漏洞源于缺乏对用户提供的数据的正确验证，这可能导致不信任数据的反序列化。。

参考链接：https://securityaffairs.co/wordpress/112370/security/hpe-flaw-systems-insight-manager.html

2. 300 万用户安装了 28 个 Chrome 或 Edge 恶意扩展程序

安全公司 Avast 表示，超过三百万的互联网用户已经安装了 15 个 Chrome 和 13 个包含恶意代码的 Edge 扩展程序。这 28 个扩展包含可能执行若干恶意操作的代码。此活动的主要目的是劫持用户流量以谋取钱财。

参考链接：https://www.zdnet.com/article/three-million-users-installed-28-malicious-chrome-or-edge-extensions/

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