国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 06 月 29 日-2020 年 07 月 05 日　　2020 年第 27 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 400 个，其中高危漏洞 83 个、中危漏洞 263 个、低危漏洞 54 个。漏洞平均分值为 5.46。本周收录的漏洞中，涉及 0day 漏洞 49 个（占 12%），其中互联网上出现“Tenda D301 跨站脚本漏洞、Triologic Media Player 缓冲区溢出漏洞”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 2924 个，与上周（3522 个）环比减少 17%。

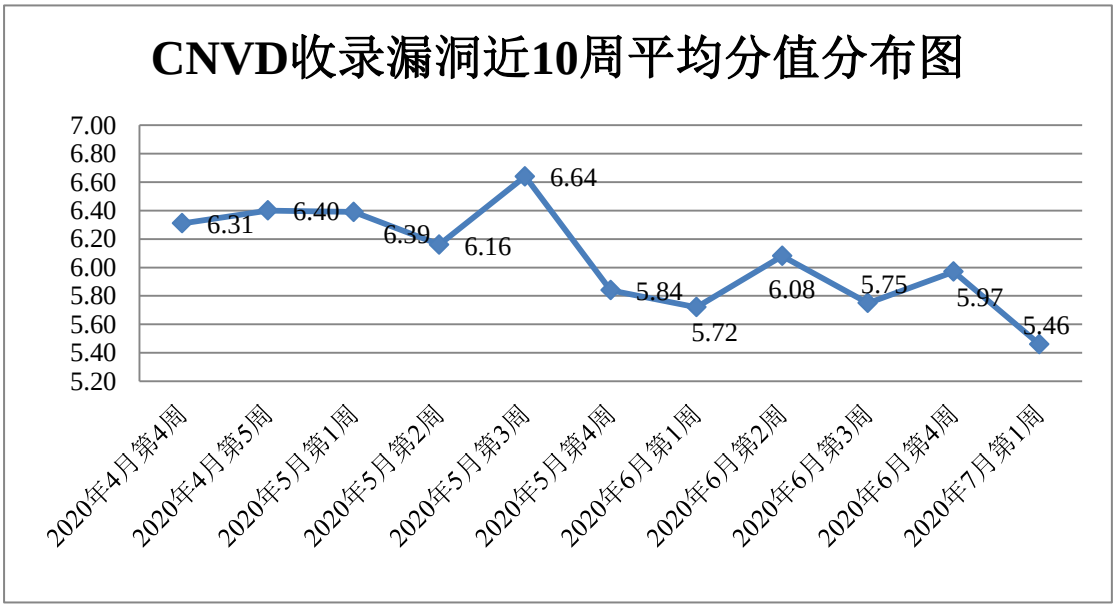

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 5 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 271 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 53 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 24 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：

北京东华原医疗设备有限责任公司、深圳市圆梦云科技有限公司、金华市亿途网络科技有限公司、杭州贝腾科技有限公司、青岛灼灼文化传媒有限公司、深圳勤杰软件有限公司、宿迁鑫潮信息技术限公司、研华科技（中国）有限公司、青岛易企天创管理咨询有限公司、苏州托普斯网络科技有限公司、北京清科锐华软件有限公司、杭州达勒网络信息技术有限公司、深圳市锟铻科技有限公司、重庆匠果科技有限公司、上海梦之路数字科技有限公司、石家庄易方得普科技开发有限公司、小米科技有限责任公司、苏宁易购集团股份有限公司、北京美特软件技术有限公司、上海同道信息技术有限公司、廊坊市极致网络科技有限公司 、北京二六三企业通信有限公司、深圳齐心好视通云计算有限公司、武汉富思特创新信息技术有限公司、广东凯格科技有限公司、北京金盘鹏图软件技术有限公司、连云港三众软件科技有限公司、宁波华硕网络服务有限公司、廊坊市极致网络科技有限公司、宁波勇冠网络科技有限公司、湖北国昇科技有限公司、厦门得推网络科技有限公司、南昌蓝智科技有限公司、校无忧科技网络公司、合肥启凡网络科技有限公司、广州市问途信息技术有限公司、哈尔滨鸿孚科技发展有限公司、合肥一浪网络科技有限公司、魁网科技（重庆）有限公司、太原迅易科技有限公司、镇江市云优网络科技有限公司、珠海金山办公软件有限公司、汕头市网蚁网络有限公司、上海布谷网络科技有限公司、广州市三今网络技术有限公司、海南易而优科技有限公司、无锡新互动网络科技有限公司、深圳市金视电子科技有限公司、济南卓源软件有限公司、合肥彼岸互联信息技术有限公司、上海宽娱数码科技有限公司、大连龙采科技开发有限公司、西安时光科技发展有限公司、杭州兆臻网络科技有限公司、海南赞赞网络科技有限公司、无锡时光网络科技有限公司、石家庄市征红网络科技有限公司、青岛商至信网络科技有限公司、贵阳思普信息技术有限公司、安徽省科大奥锐科技有限公司、成都依能科技股份有限公司、淄博旭冉网络科技有限公司、宁波鄞州子曰网络科技有限公司、河南中钰网络科技有限公司、金华市激石信息技术有限公司、普联技术有限公司、深圳市中联创新自控系统有限公司、淮安叉叉网络科技有限公司、山西龙采科技有限公司、广州市创科网络科技有限公司、南京广推网络科技有限公司、保定市互动企业营销策划有限公司、吉林安徒文化传播有限公司、茉柏枘（上海）软件科技有限公司、浙江宇视科技有限公司、上海点芮网络科技有限公司、深圳市博思协创网络科技有限公司、Lerx 网络科技、网展科技、校无忧科技、中国电子标准协会培训中心、沈阳市皇姑区爱浓网络技术服务中心、广州市花都区新华伟创广告设计服务部、上海荃路软件开发工作室、伟创互联网络技术开发团队、华科网络技术开发、魔方动力、推券客联盟、阿江守候、提拉米苏表白墙、施耐德（Schneider Electric）、ZBlogger 社区、UCMS、Heybbs、Shop7z、

115CMS、Emlog 和 lzcms。

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、恒安嘉新(北京)科技股份公司、哈尔滨安天科技集团股份有限公司、北京奇虎科技有限公司、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。长春嘉诚信息技术股份有限公司、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、山东道普测评技术有限公司、河南灵创电子科技有限公司、北京云科安信科技有限公司、杭州迪普科技股份有限公司、国瑞数码零点实验室、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、广西网信信息技术有限公司、国网山东省电力公司、北京天地和兴科技有限公司、河南信安世纪科技有限公司、上海观安信息技术股份有限公司、内蒙古奥创科技有限公司、河北华测信息技术有限公司、北京圣博润高新技术股份有限公司、京东云安全、内蒙古洞明科技有限公司、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、北京顶象技术有限公司、星云博创科技有限公司、北京智游网安科技有限公司、北京信联科汇科技有限公司、浙江宇视科技有限公司、广州安亿信软件科技有限公司、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 2924 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 1820 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）	754	754
奇安信网神（补天平台）	709	709
北京天融信网络安全技术有限公司	398	11
上海交大	357	357
恒安嘉新(北京)科技股份公司	260	0
哈尔滨安天科技集团股份有限公司	246	0
北京奇虎科技有限公司	164	118
新华三技术有限公司	163	0
深信服科技股份有限公司	115	0

华为技术有限公司	94	0
北京神州绿盟科技有限公司	88	8
北京数字观星科技有限公司	37	0
北京知道创宇信息技术股份有限公司	8	5
北京安信天行科技有限公司	4	4
中国电信集团系统集成有限责任公司	2	2
南京铱迅信息技术股份有限公司	1	1
长春嘉诚信息技术股份有限公司	121	121
山东新潮信息技术有限公司	61	61
远江盛邦（北京）网络安全科技股份有限公司	50	50
山东道普测评技术有限公司	47	47
河南灵创电子科技有限公司	28	28
北京云科安信科技有限公司	20	20
杭州迪普科技股份有限公司	15	0
国瑞数码零点实验室	9	9
南京众智维信息科技有限公司	8	8
山东云天安全技术有限公司	6	6
广西网信信息技术有限公司	6	6
国网山东省电力公司	6	6
北京天地和兴科技有限公司	6	6
河南信安世纪科技有限公司	5	5
上海观安信息技术股份有限公司	5	5

内蒙古奥创科技有限公司	3	3
河北华测信息技术有限公司	3	3
北京圣博润高新技术股份有限公司	3	3
京东云安全	3	3
内蒙古洞明科技有限公司	2	2
北京华云安信息技术有限公司	2	2
山东华鲁科技发展股份有限公司	2	2
北京顶象技术有限公司	1	1
星云博创科技有限公司	1	1
北京智游网安科技有限公司	1	1
北京信联科汇科技有限公司	1	1
浙江宇视科技有限公司	1	1
广州安亿信软件科技有限公司	1	1
上海纽盾科技股份有限公司	1	1
CNCERT 海南分中心	16	16
CNCERT 河北分中心	8	8
CNCERT 上海分中心	5	5
CNCERT 贵州分中心	5	5
CNCERT 宁夏分中心	5	5
CNCERT 黑龙江分中心	5	5
CNCERT 安徽分中心	4	4
CNCERT 西藏分中心	3	3
CNCERT 广西分中心	1	1

CNCERT 四川分中心	1	1
个人	499	499
报送总计	4370	2924

本周漏洞按类型和厂商统计

本周，CNVD 收录了 400 个漏洞。应用程序 258 个，WEB 应用 72 个，操作系统 32 个，网络设备（交换机、路由器等网络端设备）27 个，安全产品 6 个，智能设备（物联网终端设备）3 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	258
WEB 应用	72
操作系统	32
网络设备（交换机、路由器等网络端设备）	27
安全产品	6
智能设备（物联网终端设备）	3
数据库	2

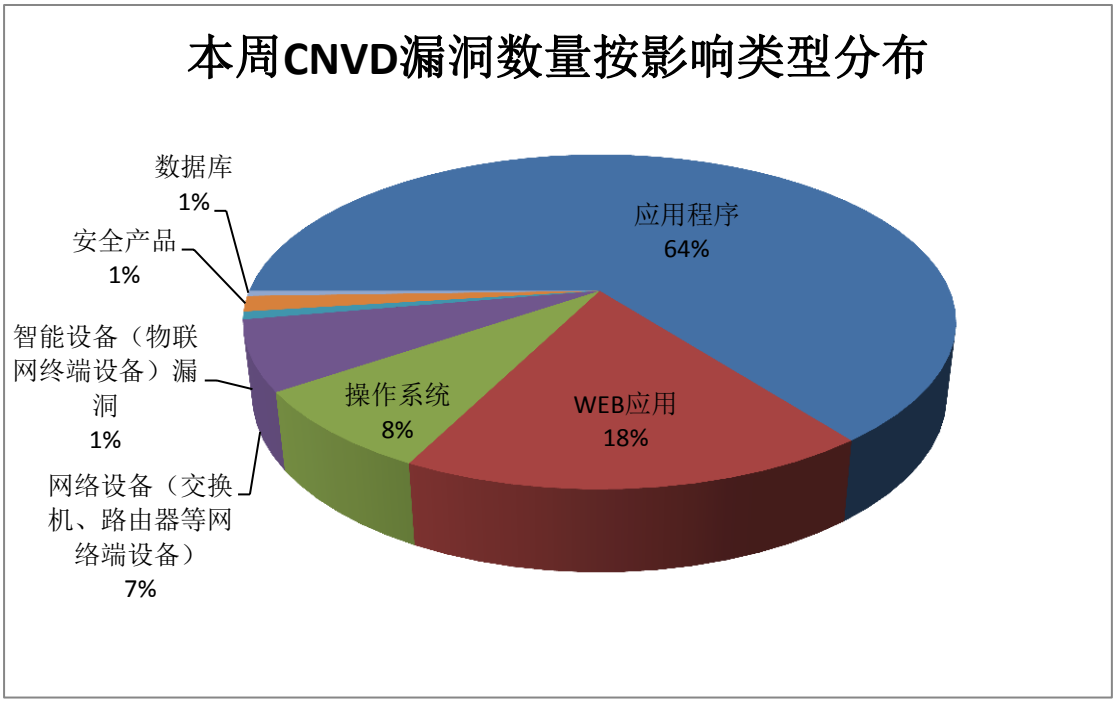

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mattermost、Google、Intel 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	Mattermost	95	23%
2	Google	17	4%
3	Intel	15	4%
4	Adobe	13	3%
5	Red Hat	12	3%
6	IBM	12	3%
7	Cisco	11	3%
8	Zephyr	11	3%
9	Naviwebs	10	3%
10	其他	204	51%

本周行业漏洞收录情况

本周，CNVD 收录了 20 个电信行业漏洞，27 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“多款 Cisco 产品缓冲区溢出漏洞（CNVD-2020-35165）、Mattermost Desktop App 访问控制错误漏洞、Citrix Systems Workspace App 权限提升漏洞、Cisco Webex Meetings 和 WebEx Meetings Server 授权问题漏洞、Mattermost Desktop App 代码注入漏洞”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/

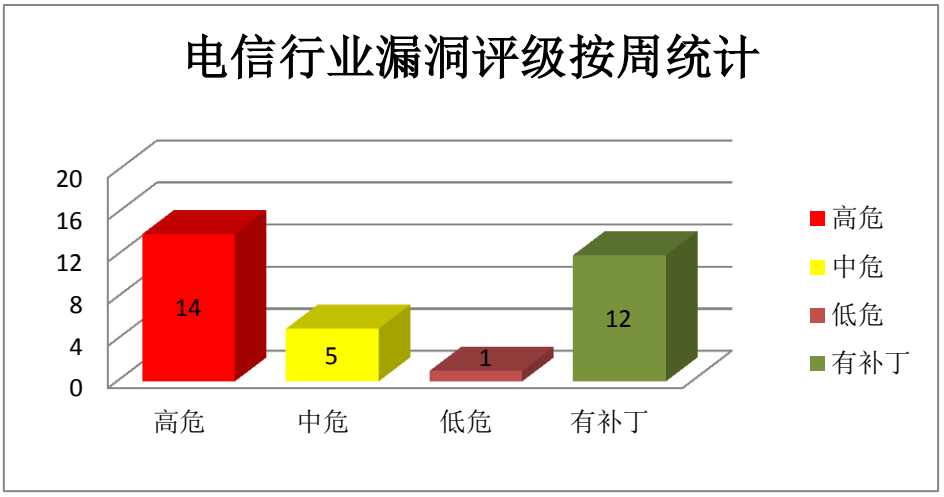

图 3 电信行业漏洞统计

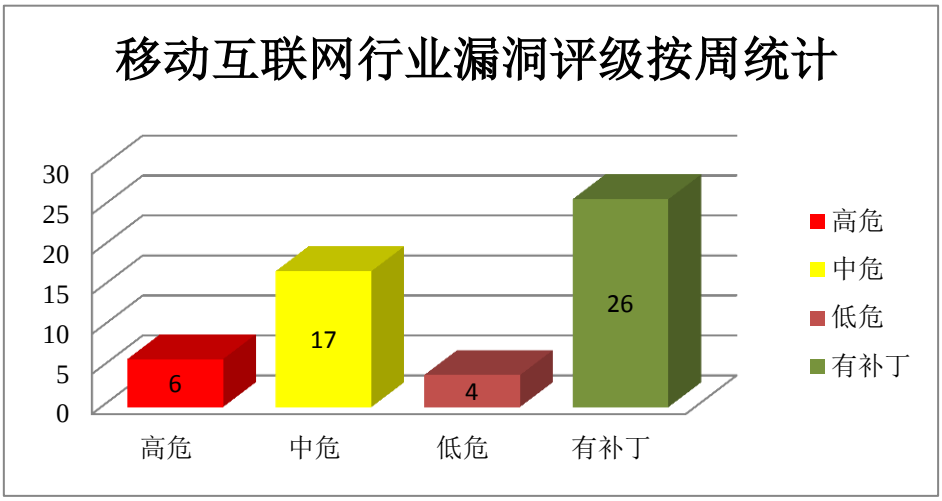

图 4 移动互联网行业漏洞统计

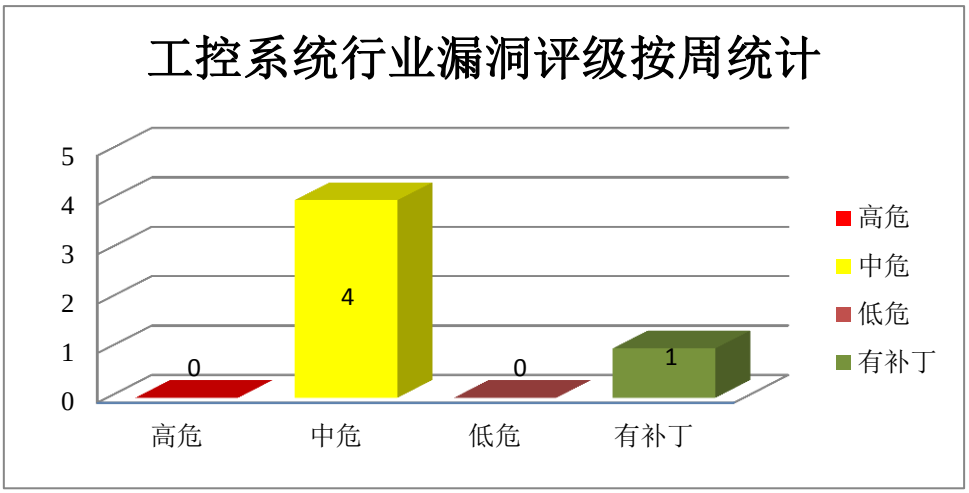

图 5 工控系统行业漏洞统计

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、 Adobe 产品安全漏洞

Adobe Illustrator 是一套基于向量的图像制作软件。Adobe After Effects 是一套视觉效果和动态图形制作软件。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Illustrator 缓冲区溢出漏洞（CNVD-2020-36219、CNVD-2020-36222、CNVD-2020-36221、CNVD-2020-36220）、Adobe After Effects 缓冲区溢出漏洞（CNVD-2020-36225、CNVD-2020-36224、CNVD-2020-36227、CNVD-2020-36226）。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-2020-36219

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36222

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36221

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36220

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36225

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36224

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36227

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36226

2、Cisco 产品安全漏洞

Cisco Small Business RV320 等都是美国思科（Cisco）公司的一款 VPN 路由器。Cisco RV110W 等都是美国思科（Cisco）公司的一款 VPN 防火墙路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以 root 权限执行任意命令。

CNVD 收录的相关漏洞包括：多款 Cisco 产品命令注入漏洞（CNVD-2020-35159、CNVD-2020-35161、CNVD-2020-35160、CNVD-2020-35162、CNVD-2020-35163、CNVD-2020-35166）、多款 Cisco 产品缓冲区溢出漏洞（CNVD-2020-35165、CNVD-2020-35167）。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-2020-35159

https://www.cnvd.org.cn/flaw/show/CNVD-2020-35161

https://www.cnvd.org.cn/flaw/show/CNVD-2020-35160

https://www.cnvd.org.cn/flaw/show/CNVD-2020-35162

https://www.cnvd.org.cn/flaw/show/CNVD-2020-35163

https://www.cnvd.org.cn/flaw/show/CNVD-2020-35166

https://www.cnvd.org.cn/flaw/show/CNVD-2020-35165

https://www.cnvd.org.cn/flaw/show/CNVD-2020-35167

3、IBM 产品安全漏洞

IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。IBM Security Secret Server 是一套特权访问管理解决方案。IBM Spectrum Protect Plus 是一套数据保护平台。IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。IBM MQ（IBM WebSphere 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，造成拒绝服务（段错误）等。

CNVD 收录的相关漏洞包括：IBM Maximo Asset Management SQL 注入漏洞（CNVD-2020-34981、CNVD-2020-34982）、IBM Security Secret Server 信息泄露漏洞（CNVD-2020-34984、CNVD-2020-34985）、IBM Spectrum Protect Plus 信息泄露漏洞（C

NVD-2020-34983）、IBM MQ 和 IBM MQ Appliance 信任管理问题漏洞、IBM MQ 拒绝服务漏洞（CNVD-2020-34988）、IBM MQ 权限提升漏洞（CNVD-2020-35725）。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-2020-34981
https://www.cnvd.org.cn/flaw/show/CNVD-2020-34984
https://www.cnvd.org.cn/flaw/show/CNVD-2020-34983
https://www.cnvd.org.cn/flaw/show/CNVD-2020-34982
https://www.cnvd.org.cn/flaw/show/CNVD-2020-34985
https://www.cnvd.org.cn/flaw/show/CNVD-2020-34989
https://www.cnvd.org.cn/flaw/show/CNVD-2020-34988
https://www.cnvd.org.cn/flaw/show/CNVD-2020-35725

4、Intel 产品安全漏洞

Intel Active Management Technology（AMT）是一套以硬件为基础的计算机远程主动管理技术软件。Intel Converged Security and Management Engine（CSME）是一款安全管理引擎。Intel TXE 是一款使用在 CPU（中央处理器）中具有硬件验证功能的信任执行引擎。Intel PROSet/Wireless WiFi Software 是一款无线网卡驱动程序。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，导致拒绝服务。

CNVD 收录的相关漏洞包括：Intel AMT 输入验证错误漏洞（CNVD-2020-35708CNVD-2020-35710）、Intel CSME 输入验证错误漏洞、Intel CSME 缓冲区溢出漏洞（CNVD-2020-35715、CNVD-2020-35716）、Intel AMT 信息泄露漏洞、Intel TXE 权限提升漏洞、Intel PROSet/Wireless WiFi Software 权限提升漏洞。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-2020-35708
https://www.cnvd.org.cn/flaw/show/CNVD-2020-35711
https://www.cnvd.org.cn/flaw/show/CNVD-2020-35710
https://www.cnvd.org.cn/flaw/show/CNVD-2020-35715
https://www.cnvd.org.cn/flaw/show/CNVD-2020-35714
https://www.cnvd.org.cn/flaw/show/CNVD-2020-35718
https://www.cnvd.org.cn/flaw/show/CNVD-2020-35716
https://www.cnvd.org.cn/flaw/show/CNVD-2020-35896

5、GE Mark VIe Controller 信任管理问题漏洞

GE Mark VIe Controller 是美国通用电气（GE）公司的一套工业集成控制系统。本周，GE Mark VIe Controller 被披露存在信任管理问题漏洞。攻击者可利用该漏洞以 r

oot 权限访问控制器。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-2020-35481

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-2020-35359	Mattermost Desktop App 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://mattermost.com/security-updates/
CNVD-2020-35378	Raonwiz Dext5.ocx ActiveX 任意文件下载漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.dext5.com/page/support/notice_view.aspx?pSeq=26
CNVD-2020-35392	HPE Smart Update Manager 访问限制绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbmu03997en_us
CNVD-2020-35394	Huawei OceanStor 5310 拒绝服务漏洞	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.huawei.com/cn/psirt/security-advisories/huawei-sa-20200429-01-invalidpointer-cn
CNVD-2020-35400	TP-Link NC260 和 NC450 操作系统命令注入漏洞	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.tp-link.com/
CNVD-2020-35674	Mozilla Firefox 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2020-16/
CNVD-2020-35683	BMC Software Control-M/Agent 命令执行漏洞	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.bmcsoftware.de/
CNVD-2020-35934	SAP Commerce 信任管理问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=547426775
CNVD-2020-35946	Citrix Systems Workspace App 权限提升漏洞	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.citrix.com/downloads/workspace-app/workspace-app-for-windows-long-term-service-release/workspace-app-for-windows-1912ltsr.html
CNVD-2020-35958	Apache Unomi 输入验证错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://unomi.apache.org/security/cve-2020-11975.txt

小结：本周，Adobe 产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。此外，Cisco、IBM、Intel 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，提升权限，执行任意命令，导致拒绝服务等。另外，GE Mark VIe Controller 被披露存在信任管理问题漏洞。攻击者可利用该漏洞以 root 权限访问控制器。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、Tenda D301 跨站脚本漏洞

验证描述

Tenda D301 是中国腾达（Tenda）公司的一款无线路由器。

Tenda D301 v2 版本中存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：https://www.exploit-db.com/exploits/47107

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-35173

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. PAN OS 操作系统曝“10 分”罕见漏洞，需立即修复

美国网络司令部发布 Twitter：“请立即修补受 CVE-2020-2021 影响的所有设备，尤其是在使用 SAML 的情况下。”特殊的是，这是一个罕见地在 CVSS v3 漏洞严重等级中获得满分 10 分的身份验证绕过漏洞，允许攻击者无需提供有效凭据即可访问设备。

参考链接：https://www.freebuf.com/news/241526.html

2. UPnP 协议 CallStranger 漏洞影响数百万设备

2020 年 6 月 8 日，安全研究员 Yunus Çadirci 公布 UPnP（通用即插即用）协议漏洞公告（CVE-2020-12695），并将其命名为 CallStranger 漏洞。该漏洞允许攻击者绕过内网的数据防泄露系统（DLP）进行数据逃逸，可导致敏感数据泄露，并且可对设备所在内部网络进行扫描，甚至能劫持设备进行分布式拒绝服务（DDOS）攻击。根据 CallStranger 漏洞原理，启明星辰 ADLab 以某款智能电视作为测试目标，对 CallStranger 漏洞的危害性进行了演示分析。

参考链接：https://paper.seebug.org/1258/

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