国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 08 月 10 日-2020 年 08 月 16 日　　2020 年第 33 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 301 个，其中高危漏洞 124 个、中危漏洞 158 个、低危漏洞 19 个。漏洞平均分值为 6.27。本周收录的漏洞中，涉及 0day 漏洞 176 个（占 58%），其中互联网上出现“Travel Management System SQL 注入漏洞、OpenEMR 'controller'远程代码执行漏洞”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 3721 个，与上周（4221 个）环比减少 12%。

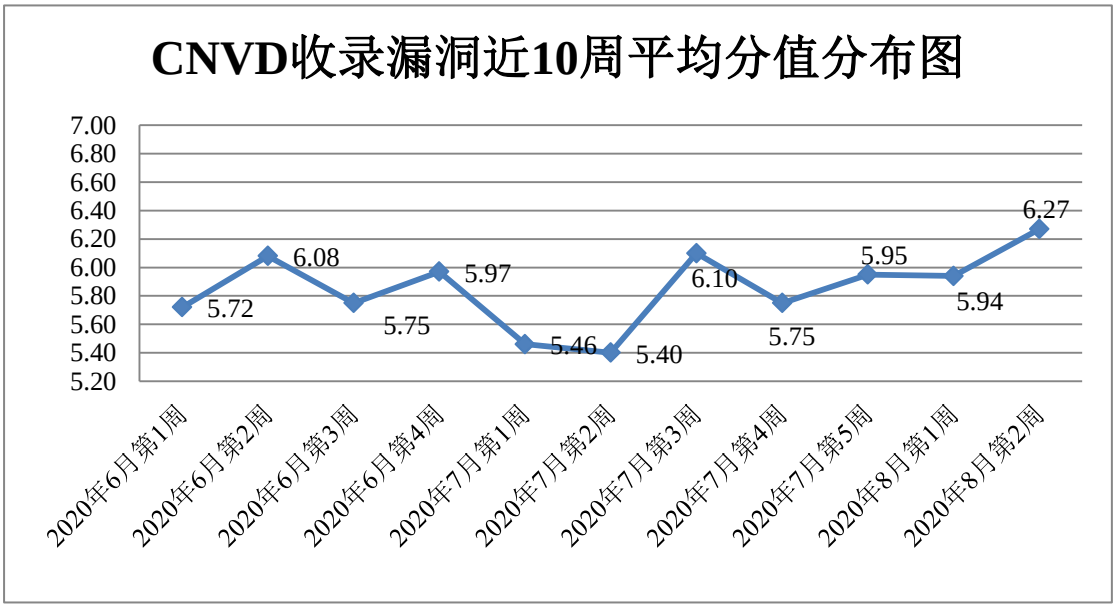

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 29 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 284 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 64 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 44 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：

北京通达信科科技有限公司、长沙米拓信息技术有限公司、星际（杭州）网络技术有限公司、四平市九州易通科技有限公司、上海七慧网络科技有限公司、西安嘉客信息科技有限责任公司、美图公司、深圳市微客互动有限公司、江西类友网络科技有限公司、陕西金博瑞网络科技有限公司、苏州汇川技术有限公司、温州乔宇科技有限公司、深圳市硕赢互动信息技术有限公司、沈阳数业信息技术有限公司、珠海金山办公软件有限公司、辽宁格瑞帕洛孚新能源有限公司、西安紫云羚网络科技有限责任公司、深圳市天视通电子科技有限公司、深圳搜豹网络有限公司、青岛东胜伟业软件有限公司、淮南润成科技股份有限公司、厦门四信通信科技有限公司、领航未来（北京）科技有限公司、北京卓研科技有限公司、宜兴易发网络服务有限公司、淄博闪灵网络科技有限公司、畅捷通信息技术股份有限公司、重庆满荣网络技术有限公司、浙江浙大中控信息技术有限公司、深圳市中采亿合科技有限公司、浙江大华技术股份有限公司、深圳方维网络科技有限公司、上海师廉网络科技发展有限公司、常州微诺信息科技有限公司、苏州思迪信息技术有限公司、深圳华磊物流通信息科技有限公司、北京中成科信科技发展有限公司、润申信息科技（上海）有限公司、南昌正能信息技术有限公司、漳州市芗城帝兴软件开发有限公司、湖南谱典信息技术有限公司、苏州推广家网络科技有限公司、汉王科技股份有限公司、北京转折文化发展有限公司、汉中市启元动力网络有限公司、海南易而优科技有限公司、深圳市锟铻科技有限公司、深圳神州通达网络技术有限公司、青岛易企天创管理咨询有限公司、广东凯格科技有限公司、上海智休信息科技有限公司、厦门凤凰创壹软件有限公司、汉中启元动力网络有限公司、上海昊沧系统控制技术有限责任公司、台湾宜蘭民宿旅游网、北京为因软件、帝国软件、小京鱼智能服务平台、乐尚商城开源系统、梦想 CMS、ZBlogger 社区、鱼跃 CMS、DocCms X 开发团队、The Apache Software Foundation、CLTPHP、nideshop、ThinkSAAS 和 yccms。

本周，CNVD 发布了《Microsoft 发布 2020 年 8 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5617

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、华为技术有限公司、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、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。国瑞数码零点实验室、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、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、山东道普测评技术有限公司、北京华云安信息技术有限公司、河南灵创电子科技有限公司、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、浙江宇视科技有限公司、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、河南信安世纪科技有限公司、广州三零卫士信息安全有限公司、北京长亭科技有限公司、长春嘉诚信息技术股份有限公司、杭州安信检测技术有限公司、北京禹宏信安科技有限公司、平安银河实验室、北京智游网安科技有限公司、河北千诚电子科技有限公司、上海观安信息技术股份有限公司、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 3721 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 2666 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）	1301	1301
斗象科技（漏洞盒子）	986	986
上海交大	379	379
北京神州绿盟科技有限公司	319	9
华为技术有限公司	251	0
北京天融信网络安全技术有限公司	224	25
哈尔滨安天科技集团股份有限公司	222	0
新华三技术有限公司	112	0
深信服科技股份有限公司	94	0
北京启明星辰信息安全技术有限公司	59	0
浙江大华技术股份有限公司	12	12
北京安信天行科技有限公司	7	7
北京知道创宇信息技术股份有限公司	3	0
沈阳东软系统集成工程有限公司	2	2

国瑞数码零点实验室	137	137
北京云科安信科技有限公司（Seraph 安全实验室）	110	110
远江盛邦（北京）网络安全科技股份有限公司	65	65
山东华鲁科技发展股份有限公司	46	46
山东新潮信息技术有限公司	41	41
山东道普测评技术有限公司	36	36
北京华云安信息技术有限公司	30	30
河南灵创电子科技有限公司	23	23
杭州迪普科技股份有限公司	14	0
南京众智维信息科技有限公司	13	13
山东云天安全技术有限公司	12	12
西门子（中国）有限公司	8	0
浙江宇视科技有限公司	8	8
安徽长泰信息安全服务有限公司	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	6	6
广州三零卫士信息安全有限公司	5	5
北京长亭科技有限公司	3	3
长春嘉诚信息技术股份有限公司	3	3
杭州安信检测技术有限公司	3	3
北京禹宏信安科技有限公司	2	2
平安银河实验室	2	2

北京智游网安科技有限公司	1	1
河北千诚电子科技有限公司	1	1
上海观安信息技术股份有限公司	1	1
四川哨兵信息科技有限公司	1	1
CNCERT 四川分中心	4	4
CNCERT 西藏分中心	2	2
CNCERT 贵州分中心	1	1
CNCERT 青海分中心	1	1
个人	431	431
报送总计	4993	3721

本周漏洞按类型和厂商统计

本周，CNVD 收录了 301 个漏洞。WEB 应用 145 个，应用程序 100 个，操作系统 38 个，网络设备（交换机、路由器等网络端设备）17 个，智能设备（物联网终端设备）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
WEB 应用	145
应用程序	100
操作系统	38
网络设备（交换机、路由器等网络端设备）	17
智能设备（物联网终端设备）	1

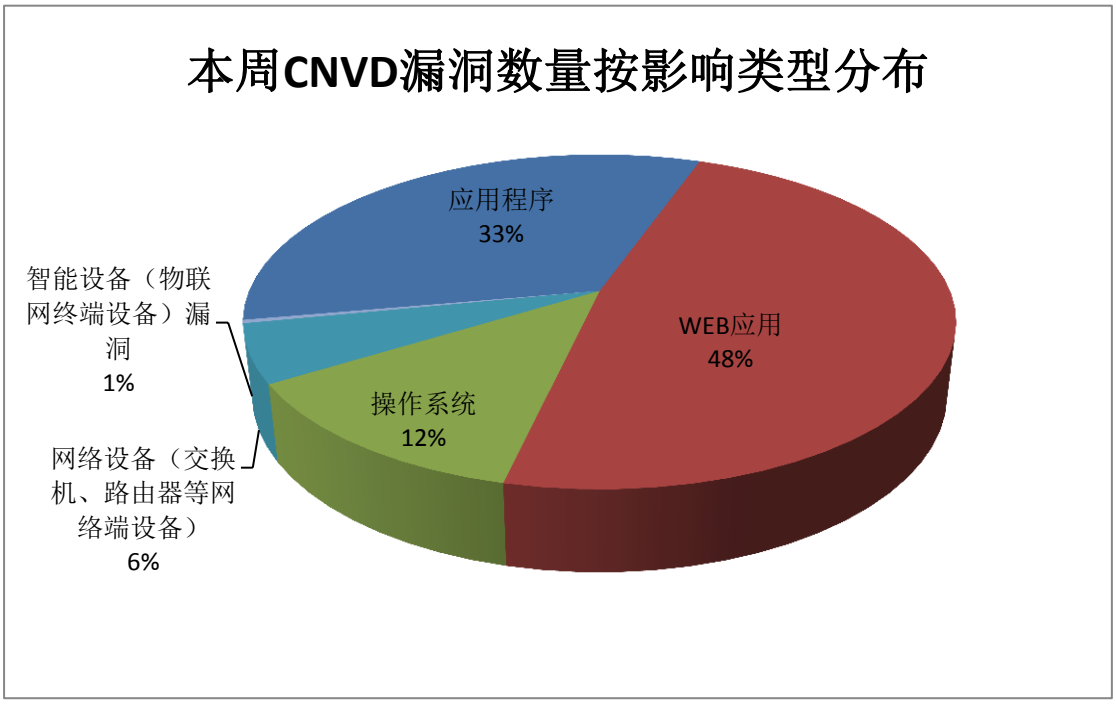

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Google、Artifex Software 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	Adobe	27	9%
2	Google	24	8%
3	Artifex Software	23	8%
4	Microsoft	23	8%
5	海南椰角网络科技有限公司	21	7%
6	Apache	10	3%
7	Cisco	8	3%
8	内蒙古万户信息科技有限公司	5	2%
9	Foxit	4	1%
10	其他	156	51%

本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，36 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“Siemens Desigo CC 和 Desigo CC Compact 代码注入漏

洞、Siemens Automation License Manager 本地权限提升漏洞、NETGEAR R6700 栈缓冲区溢出漏洞、Google Android Kernel Airbrush 资源管理错误漏洞”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/

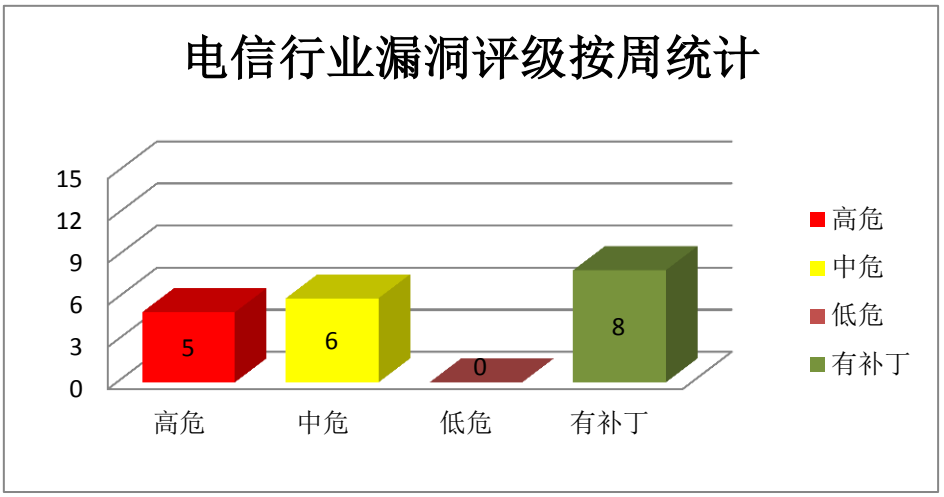

图 3 电信行业漏洞统计

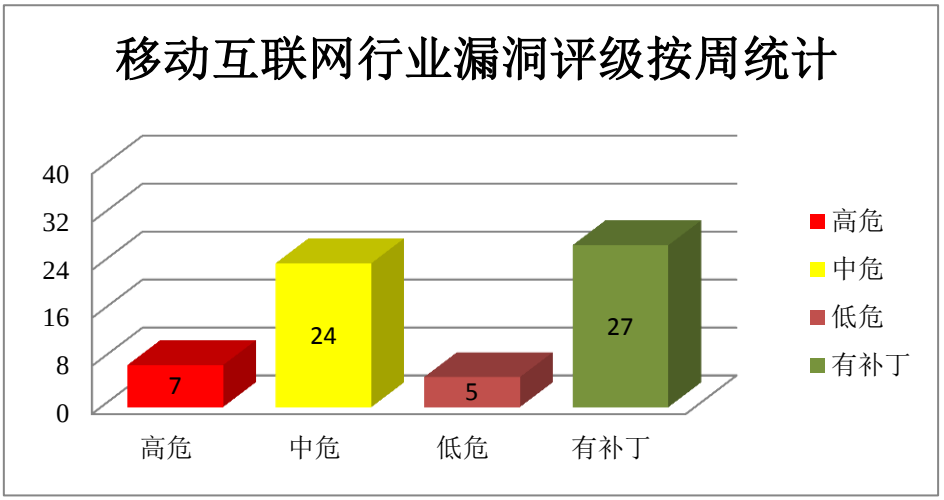

图 4 移动互联网行业漏洞统计

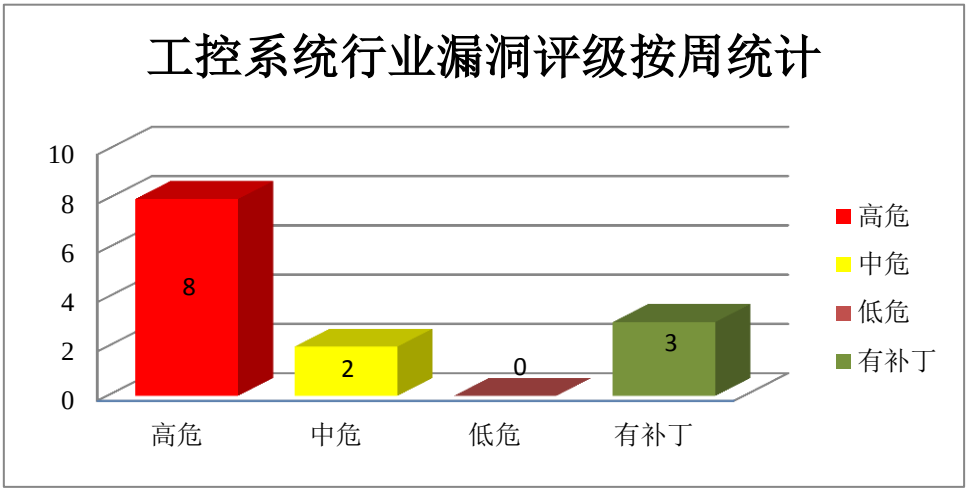

图 5 工控系统行业漏洞统计

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 Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。Adobe Acrobat 是一款 PDF 编辑软件。本周，上述产品被披露存在越界读取漏洞，攻击者可利用漏洞获取信息。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 越界读取漏洞（CNVD-2020-46036、CNVD-2020-46035、CNVD-2020-46039、CNVD-2020-46038、CNVD-2020-46037、CNVD-2020-46041、CNVD-2020-46040、CNVD-2020-46043）。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-2020-46036
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46035
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46039
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46038
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46037
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46041
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46040
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46043

2、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 Excel 是一款 Office 套件中的电子表格处理软件。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，执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Windows ALPC 权限提升漏洞、Microsoft Excel 缓冲区溢出漏洞（CNVD-2020-45184）、Microsoft Hyper-V RemoteFX vGPU 缓冲区溢出漏洞（CNVD-2020-45325、CNVD-2020-45324、CNVD-2020-45323）、Microsoft Windows Hyper-V RemoteFX vGPU 输入验证错误漏洞、Microsoft Windows Hyper-V RemoteFX vGPU 远程代码执行漏洞、Microsoft Hyper-V RemoteFX vGPU 资源管理错误漏洞。其中，除“Microsoft Windows ALPC 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-2020-45187
https://www.cnvd.org.cn/flaw/show/CNVD-2020-45184
https://www.cnvd.org.cn/flaw/show/CNVD-2020-45325
https://www.cnvd.org.cn/flaw/show/CNVD-2020-45324
https://www.cnvd.org.cn/flaw/show/CNVD-2020-45323
https://www.cnvd.org.cn/flaw/show/CNVD-2020-45328
https://www.cnvd.org.cn/flaw/show/CNVD-2020-45327
https://www.cnvd.org.cn/flaw/show/CNVD-2020-45326

3、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，攻击者可利用漏洞获取信息，提升权限，执行代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android Media Framework 权限提升漏洞（CNVD-2020-46237）、Google Android Framework 缓冲区溢出漏洞（CNVD-2020-46263）、Google Android Media Framework 信息泄露漏洞（CNVD-2020-46266、CNVD-2020-46265）、Google Android Media Framework 资源管理错误漏洞（CNVD-2020-46264）、Google Android Media Framework 缓冲区溢出漏洞（CNVD-2020-46267）、Google Android Media Framework 拒绝服务漏洞（CNVD-2020-46272）、Google Android Framework 越界读取漏洞。其中，“Google Android Media Framework 权限提升漏洞（CNVD-2020-46237）”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-2020-46237
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46263
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46266
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46265
https://www.cnvd.org.cn/flaw/show/CNVD-2020-46264

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46267

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46272

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46270

4、Apache 产品安全漏洞

Apache Tomcat 是一款轻量级 Web 应用服务器。Apache HTTP Server 是一款开源网页服务器。Struts2 是 Apache 软件基金会负责维护的一个基于 MVC 设计模式的 Web 应用框架开源项目。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信息，执行任意代码，造成拒绝服务（无限循环）等。

CNVD 收录的相关漏洞包括：Apache Struts2 S2-059 远程代码执行漏洞、Apache Struts2 S2-060 拒绝服务漏洞、Apache Tomcat 资源管理错误漏洞（CNVD-2020-46233）、Apache Tomcat 代码问题漏洞、Apache Tomcat 拒绝服务漏洞（CNVD-2020-46230）、Apache HTTP Server 数据伪造问题漏洞、Apache HTTP Server 环境问题漏洞、Apache HTTP Server 缓冲区溢出漏洞。其中，“Apache Struts2 S2-059 远程代码执行漏洞、Apache Struts2 S2-060 拒绝服务漏洞、Apache HTTP Server 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-2020-46202

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46201

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46233

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46232

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46230

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46278

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46281

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46280

5、Cisco 7947G 权限提升漏洞

Cisco 7947G 是美国思科（Cisco）公司的一款在线会议终端设备。本周，Cisco 7947G 被披露存在权限提升漏洞。攻击者可利用该漏洞提升权限。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-2020-46238

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-2020-45699	Siemens Desigo CC 和 Desigo CC Compact 代码注入漏	高	用户可参考如下供应商提供的安全公告获得补丁信息：

	洞		https://cert-portal.siemens.com/productcert/pdf/ssa-786743.pdf
CNVD-2020-45323	Microsoft Hyper-V RemoteFX vGPU 缓冲区溢出漏洞（CNVD-2020-45323）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1036
CNVD-2020-45581	Cisco SD-WAN Solution 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-dos-KWOdyHnB
CNVD-2020-45701	Siemens SICAM A8000 RTU 跨站脚本漏洞	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://cert-portal.siemens.com/productcert/pdf/ssa-370042.pdf
CNVD-2020-46201	Apache Struts2 S2-060 拒绝服务漏洞	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://cwiki.apache.org/confluence/display/ww/s2-060
CNVD-2020-46224	多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2020-46224）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kb.netgear.com/000062128/Security-Advisory-for-Pre-Authentication-Stack-Overflow-on-R6700v3-PSV-2020-0224
CNVD-2020-45700	Siemens Automation License Manager 本地权限提升漏洞	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://cert-portal.siemens.com/productcert/pdf/ssa-388646.pdf
CNVD-2020-46226	NETGEAR R6700 栈缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kb.netgear.com/000062127/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-R6700v3-PSV-2020-0202
CNVD-2020-46229	IBM WebSphere Application Server 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.ibm.com/support/pages/node/6258333
CNVD-2020-46237	Google Android Media Framework 权限提升漏洞（CNVD-2020-46237）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/pixel/2020-06-01

小结：本周，Adobe 产品被披露存在越界读取漏洞，攻击者可利用漏洞获取信息。此外，Microsoft、Google、Apache 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取信息，提升权限，执行代码，造成拒绝服务（无限循环）等。另外，Cisco 7947G 被披露存在权限提升漏洞。攻击者可利用该漏洞提升权限。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、OpenEMR 'controller'远程代码执行漏洞

验证描述

OpenEMR 是 OpenEMR 社区的一套开源的医疗管理系统。该系统可用于医疗实践管理、电子医疗记录、处方书写和医疗帐单申请。

OpenEMR 'controller'存在远程代码执行漏洞。该漏洞源于程序未能正确地验证用户提交的数据。远程攻击者可通过发送恶意的请求利用该漏洞在底层操作系统上执行任意代码。

验证信息

POC 链接：https://www.exploit-db.com/exploits/48623

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-46223

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. 高通证实骁龙 DSP 漏洞可令 40%的智能手机易遭黑客入侵

高通公司已经证实在他们的智能手机芯片组中发现了一个巨大的缺陷，使手机完全暴露在黑客面前。该漏洞由 Check Point 安全公司发现，大量 Android 手机中的 Snapdragon DSP 的缺陷会让黑客窃取数据，安装难以被发现的隐藏间谍软件，甚至可以彻底将手机损坏而无法使用。

参考链接：https://www.cnbeta.com/articles/tech/1013611.htm

2. 三星“查找我的手机”功能出现漏洞，用户可能完全丢失数据

网络安全服务提供商 Char49 的安全研究员 Pedro Umbelino，在三星的“查找我的

手机”功能中发现了多个漏洞，这些漏洞可能被集中利用在三星 Galaxy Phone 上执行各种恶意活动。“查找我的手机”软件包中存在多个漏洞，最终可能导致智能手机用户完全丢失数据（恢复出厂设置），包括实时位置跟踪，电话和短信检索，电话锁定，电话解锁等。用户在设备的 Web 应用程序上执行的所有操作，都可能被恶意应用程序滥用。执行这些操作的代码路径涉及多个链接起来的漏洞。

参考链接：https://www.freebuf.com/news/246393.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