国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 02 月 10 日-2020 年 02 月 16 日　　2020 年第 7 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 609 个，其中高危漏洞 247 个、中危漏洞 300 个、低危漏洞 62 个。漏洞平均分值为 6.34。本周收录的漏洞中，涉及 0day 漏洞 155 个（占 25%），其中互联网上出现“CHIYU BF 430 TCP IP Converter 跨站脚本漏洞、nopCommerce 跨站请求伪造漏洞”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 4121 个，与上周（1729 个）环比增加 1.38 倍。

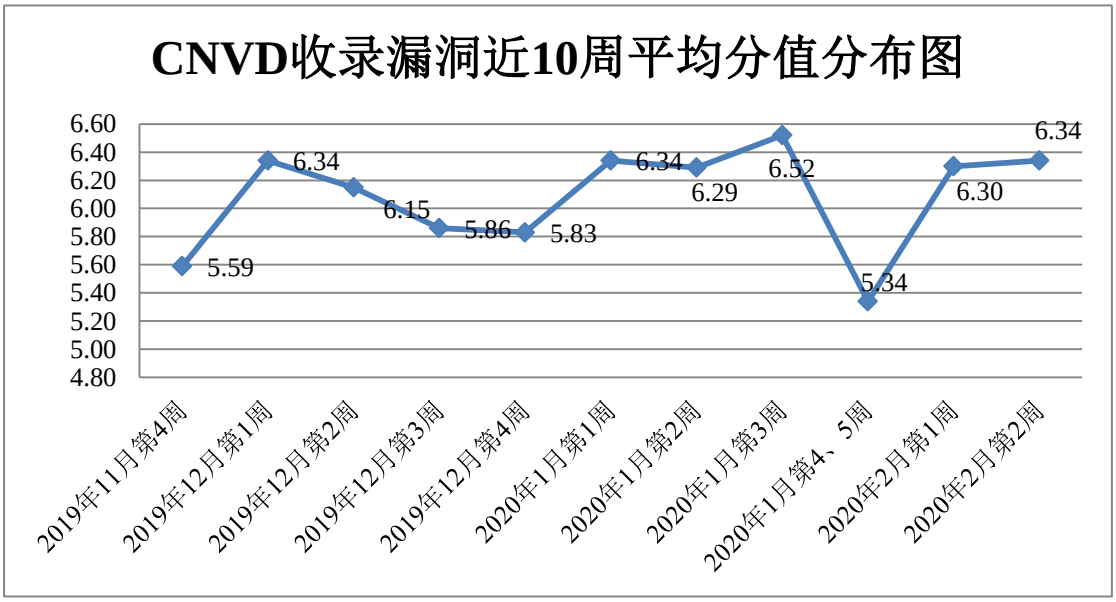

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 3 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 216 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 27 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 19 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：

南通联农农药制剂研究开发有限公司、厦门易尔通网络科技有限公司、广东卓锐软件有限公司、上海泛微网络科技股份有限公司、金蝶软件有限公司、广州购啊购科技有限公司、海南易而优科技有限公司、北京海腾时代科技有限公司、淄博闪灵网络科技有限公司、台湾永宏电机股份有限公司、呼和浩特网域科技有限责任公司、广州网易计算机系统有限公司、广州齐博网络科技有限公司、哈尔滨伟成科技有限公司、深圳市吉祥腾达科技有限公司、北京良精志诚科技有限责任公司、北京五指互联科技有限公司、中建三局集团有限公司天津分公司、山西牛酷信息科技有限公司、上海软众信息科技有限公司、湖南一唯信息科技有限公司、中国电子科技集团公司、武汉类森科技有限公司、湖南心艾网络科技有限公司、福建福昕软件开发股份有限公司、ABB 集团、中国普法教育网、BageCMS、ZhiCms、XiaoCMS、NETGEAR 和 Catfish CMS。

本周，CNVD 发布了《Microsoft 发布 2020 年 2 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5405

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、华为技术有限公司、北京神州绿盟科技有限公司、恒安嘉新(北京)科技股份公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。内蒙古洞明科技有限公司、河南灵创电子科技有限公司、北京华云安信息技术有限公司、山东云天安全技术有限公司、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、南京众智维信息科技有限公司、北京圣博润高新技术股份有限公司、厦门靠谱云股份有限公司、中科信息安全共性技术国家工程研究中心有限公司、国瑞数码零点实验室、北京长亭科技有限公司、山石网科通信技术股份有限公司、成都链安科技有限公司、成都思维世纪科技有限公司、江苏保旺达软件技术有限公司、北京小米科技有限责任公司、北京智游网安科技有限公司及其他个人白帽子向 CNVD 提交了 4121 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 1360 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）	741	741
上海交大	390	390
奇安信网神（补天平台）	229	229
北京天融信网络安全技术有限公司	188	2
华为技术有限公司	159	0
北京神州绿盟科技有限公司	82	0
恒安嘉新(北京)科技股份公司	76	0
北京启明星辰信息安全技术有限公司	50	7
新华三技术有限公司	47	0
哈尔滨安天科技集团股份有限公司	42	0
北京知道创宇信息技术股份有限公司	2	0
南京铱迅信息技术股份有限公司	1	1
厦门服云信息科技有限公司	1	1
内蒙古洞明科技有限公司	98	98
河南灵创电子科技有限公司	73	73
北京华云安信息技术有限公司	58	58
山东云天安全技术有限公司	43	43
山东新潮信息技术有限公司	38	38
远江盛邦（北京）网络安全科技股份有限公司	26	26
南京众智维信息科技有限公司	12	12
北京圣博润高新技术股份有限公司	11	11

厦门靠谱云股份有限公司	8	8
中科信息安全共性技术国家工程研究中心有限公司	6	6
国瑞数码零点实验室	5	5
北京长亭科技有限公司	3	3
山石网科通信技术股份有限公司	3	3
成都链安科技有限公司	2	2
成都思维世纪科技有限公司	2	2
江苏保旺达软件技术有限公司	2	2
北京小米科技有限责任公司	1	1
北京智游网安科技有限公司	1	1
CNCERT 重庆分中心	44	44
CNCERT 四川分中心	8	8
CNCERT 广西分中心	3	3
CNCERT 福建分中心	2	2
CNCERT 上海分中心	2	2
CNCERT 天津分中心	2	2
CNCERT 河北分中心	1	1
CNCERT 江苏分中心	1	1
CNCERT 山西分中心	1	1
CNCERT 西藏分中心	1	1
个人	2293	2293
报送总计	4758	4121

本周漏洞按类型和厂商统计

本周，CNVD 收录了 609 个漏洞。应用程序 368 个，WEB 应用 101 个，操作系统 62 个，网络设备（交换机、路由器等网络端设备）45 个，数据库 17 个，安全产品 11 个，智能设备（物联网终端设备）5 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	368
WEB 应用	101
操作系统	62
网络设备（交换机、路由器等网络端设备）	45
数据库	17
安全产品	11
智能设备（物联网终端设备）	5

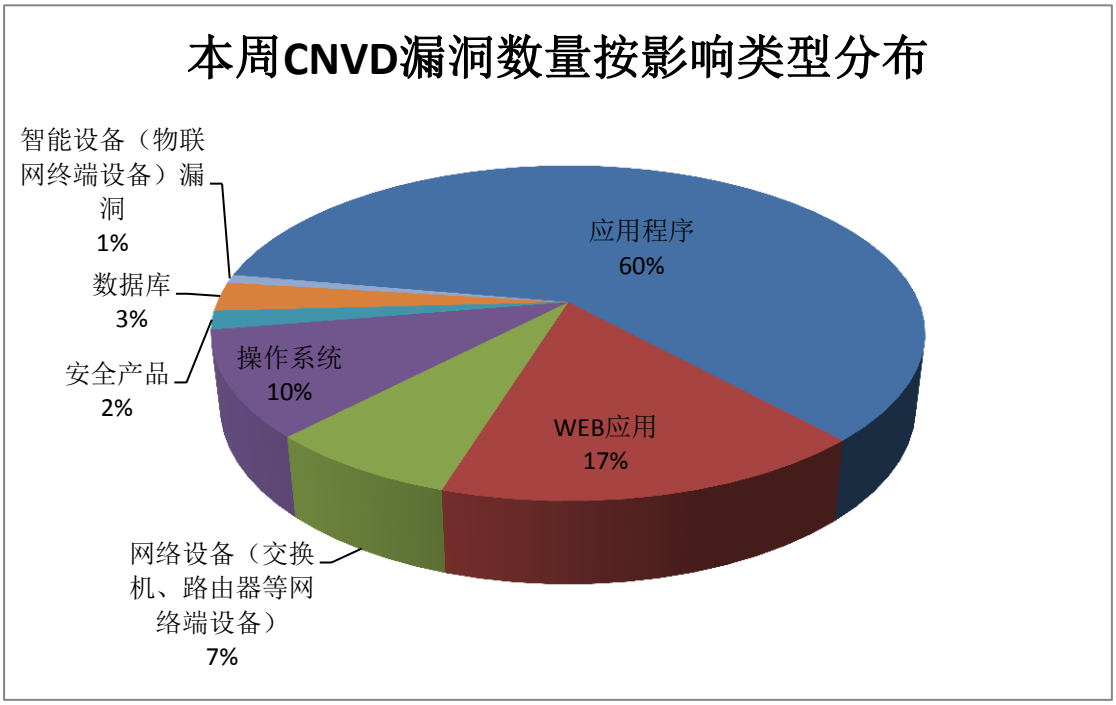

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Google、Adobe 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	Oracle	78	13%
2	Google	36	6%
3	Adobe	25	4%

4	Microsoft	23	4%
5	IBM	20	3%
6	Intel	13	2%
7	WordPress	12	2%
8	Cisco	11	2%
9	Lustre	10	2%
10	其他	381	62%

本周行业漏洞收录情况

本周，CNVD 收录了 18 个电信行业漏洞，30 个移动互联网行业漏洞，12 个工控行业漏洞（如下图所示）。其中，“SIEMENS SCALAN CES-600 family 拒绝服务漏洞、Google Android 远程代码执行漏洞（CNVD-2020-04546）、Brocade Fabric OS ESRS 敏感信息泄露漏洞、Samsung Galaxy Gear series wpa_supplicant 权限提升漏洞、GE PACSystems 输入验证错误漏洞”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/

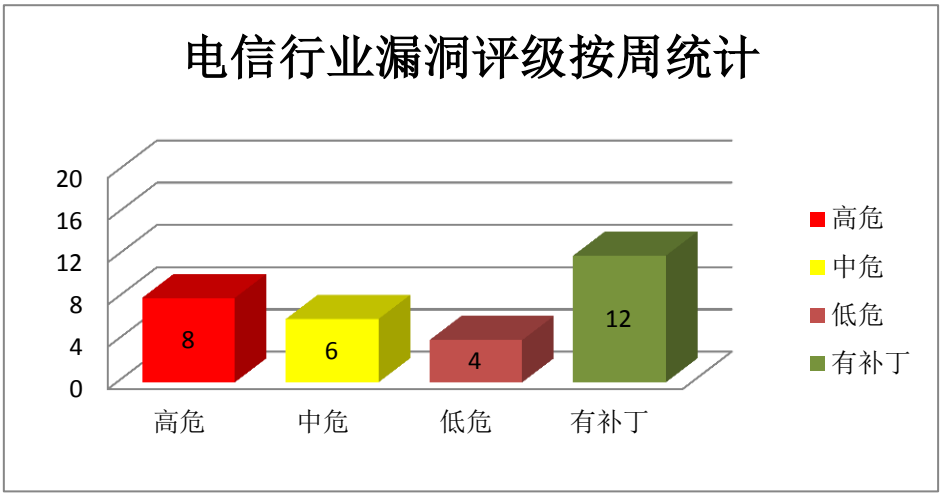

图 3 电信行业漏洞统计

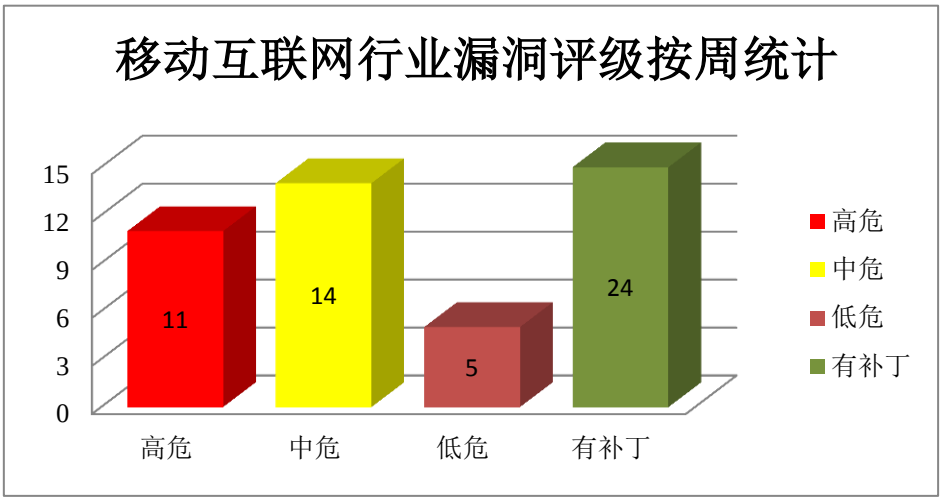

图 4 移动互联网行业漏洞统计

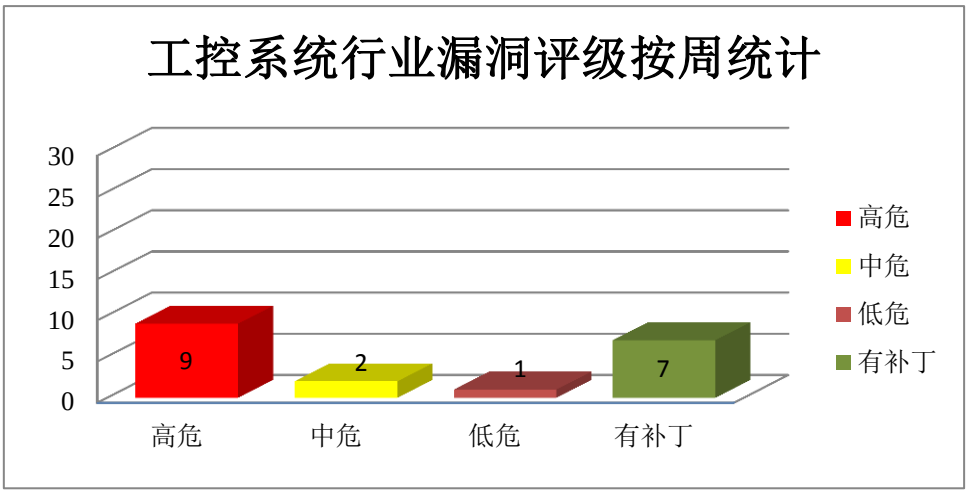

图 5 工控系统行业漏洞统计

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 FrameMaker 是一款页面排版软件。本周，上述产品被披露存在越界写入漏洞，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 FrameMaker 越界写入漏洞（CNVD-2020-08146、CNVD-2020-08147、CNVD-2020-08148、CNVD-2020-08151、CNVD-2020-08149、CNVD-2020-08150、CNVD-2020-08152、CNVD-2020-08153）。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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-08146

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08147

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08148

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08151

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08149

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08150

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08152

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08153

2、IBM 产品安全漏洞

IBM DB2 是一套关系型数据库管理系统。IBM Security Directory Server 是一套使用了轻量级目录访问协议（LDAP）的企业身份管理软件。IBM WebSphere Application Server Liberty 是一款构建于 Open Liberty 项目之上的 Java 应用程序服务器。IBM Planning Analytics 是一套业务规划分析解决方案。IBM Security Access Manager Appliance 是一款基于网络设备的安全解决方案。IBM Security Secret Server 是美国 IBM 公司的一套特权访问管理解决方案。IBM Security Identity Manager 是一套身份管理和治理解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获取敏感信息，执行任意代码，进行拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM DB2 High Performance Unload load for LUW 代码问题漏洞、IBM Security Directory Server 安全限制绕过漏洞、IBM Security Directory Server 信息泄露漏洞（CNVD-2020-04412）、IBM WebSphere Application Server 信息泄露漏洞、IBM Planning Analytics 跨站请求伪造漏洞、IBM Security Access Manager Appliance XXE 注入漏洞、IBM Security Secret 跨站脚本漏洞、IBM Security Identity Manager 目录遍历漏洞（CNVD-2020-04920）。其中，“IBM DB2 High Performance Unload load for LUW 代码问题漏洞、IBM Security Directory Server 安全限制绕过漏洞、IBM Planning Analytics 跨站请求伪造漏洞、IBM Security Access Manager Appliance XXE 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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-04410

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04408

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04412

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04414

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04416

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04545

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04912

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04920

3、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 .NET Framework 是编程模型，也是一个用于构建 Windows、Windows Store、Windows Phone、Windows Server 和 Microsoft Azure 的应用程序的开发平台。Microsoft Windows Remote Desktop Gateway 是一款基于 Windows 的远程桌面网关。Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。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。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。

CNVD 收录的相关漏洞包括：Microsoft Windows Remote Desktop Gateway 远程代码执行漏洞、Microsoft Edge 脚本引擎内存破坏漏洞（CNVD-2020-08118）、Microsoft Windows 远程代码执行漏洞（CNVD-2020-08130）、Microsoft .NET Framework 远程执行代码漏洞（CNVD-2020-08131、CNVD-2020-08132）、Microsoft Windows Common Log File System Driver 提权漏洞、Microsoft Windows Media Service 提权漏洞、Microsoft ChakraCore 和 Edge 内存破坏漏洞（CNVD-2020-08134）。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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-07950

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08118

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08130

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08131

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08132

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08133

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08135

http://www.cnvd.org.cn/flaw/show/CNVD-2020-08134

4、Intel 产品安全漏洞

Intel NUC Kit NUC7i5DNKE 是一款迷你主机产品。Intel NUC 8 Mainstream Game Kit 是一款小型台式电脑。Intel NUC 8 Mainstream Game Mini Computer 是一款小型台式电脑。Intel PROSet/Wireless WiFi Software 是一款无线网卡驱动程序。Intel Baseboard Management Controller（BMC）是一款基板管理控制器。Intel Renesas Electronics USB 是 USB 3 Renesas Electronics 适配器的驱动程序，该适配器位于许多常见的 Intel 主板中。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，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：Intel NUC 访问控制错误漏洞、Intel NUC 输入验证错误漏洞、Intel NUC 缓冲区限制错误漏洞、Intel NUC 越界写入漏洞、Intel NUC 整数溢出漏洞、Intel PROSet/Wireless WiFi Software 缓冲区溢出漏洞、Intel Baseboard Management Controller 授权问题漏洞、Intel Renesas Electronics USB 权限提漏洞。其中，

“Intel Baseboard Management Controller 授权问题漏洞、Intel Renesas Electronics USB 权限提漏洞”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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-04679

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04680

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04681

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04682

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04683

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04684

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04687

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04707

5、Red Hat Keycloak 跨站脚本漏洞

Red Hat Keycloak 是一套为现代应用和服务提供身份验证和管理功能的软件。本周，Red Hat Keycloak 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行客户端代码。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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-04661

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-2020-04509	多款 Apple 产品 Audio 组件内存破坏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/en-us/HT210722
CNVD-2020-04527	Google Android Kernel 组件权限提升漏洞（CNVD-2020-04527）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2020-02-01
CNVD-2020-04644	OSSEC-HIDS syscheck 消息拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.ossec.net/
CNVD-2020-04658	GE PACSystems 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://digitalsupport.ge.com
CNVD-2020-04706	Dell Patches SupportAssist 任意代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jira.atlassian.com/browse/JRASERVER-70564

CNVD-2020-04717	SIEMENS SCALAN CES-600 family 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://cert-portal.siemens.com/productcert/pdf/ssa-591405.pdf
CNVD-2020-04910	IBM Security Secret Server 加密问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.ibm.com/support/pages/node/1283194
CNVD-2020-05084	Apache Dubbo 反序列化漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://dubbo.apache.org/
CNVD-2020-07292	Xen 拒绝服务漏洞（CNVD-2020-07292）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://xenbits.xen.org/xsa/advisory-309.html
CNVD-2020-09648	SAP Enable Now 输入验证错误漏洞（CNVD-2020-09648）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=533660397

小结：本周，Adobe 产品被披露存在越界写入漏洞，攻击者可利用漏洞执行任意代码。此外，IBM、Microsoft、Intel 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获取敏感信息，提升权限，执行任意代码，导致缓冲区溢出或堆溢出等。另外，Red Hat Keycloak 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行客户端代码。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、CHIYU BF430 TCP IP Converter 跨站脚本漏洞

验证描述

CHIYU BF-430 是中国台湾七友科技（CHIYU）公司的一款为门禁、考勤系统等设备提供通讯的联网服务器。

CHIYU BF-430 232/485 TCP/IP Converter 1.16.00 之前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://packetstormsecurity.com/files/156289/CHIYU-BF430-TCP-IP-Converter-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-08143

信息提供者

CNVD 工作组

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. 速升 Android 10，黑客可通过旧版安卓系统蓝牙发送恶意软件

安全研究中心 ERNW 最新发布的报告称，他们发现了一个名为 BlueFrag 的漏洞，该漏洞能够允许黑客悄悄地把恶意程序通过蓝牙传送到附近的 Android 8 Oreo 和 Android 9 Pie 设备中。在 Android 8.0 到 9.0 上，只要启用了蓝牙，附近的远程攻击者就可以使用蓝牙守护程序的特权以静默方式执行任意代码。

参考链接：https://www.ithome.com/0/472/357.htm

2. Shadowsocks 流密码重定向攻击

某安全研究员披露了流行 SOCKS5 代理 Shadowsocks 的流密码重定向攻击漏洞。研究人员发现 Shadowsocks 协议存在漏洞，会破坏流密码的保密性。利用重定向攻击被动攻击者可以轻松解密所有 Shadowsocks 的加密数据包。中间人攻击者还能实时修改流量，就好像加密根本不存在。受影响的版本包括 shadowsocks-py、shadowsocoks-go 和 shadowsocoks-nodejs，shadowsocks-libev 和 go-shadowsocks2 不受影响，研究人员还建议使用 AEAD 加密算法。

参考链接：https://www.solidot.org/story?sid=63529

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