国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 08 月 12 日-2019 年 08 月 18 日 **2019 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 498 个，其中高危漏洞 167 个、中危漏洞 263 个、低危漏洞 68 个。漏洞平均分值为 5.82。本周收录的漏洞中，涉及 0day 漏洞 149 个（占 37%），其中互联网上出现“Aptana Jaxer wikilite 源码浏览器本地文件包含漏洞、Joomla!组件 com_jssupportticket 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 1469 个，与上周（1923 个）环比下降 24%。

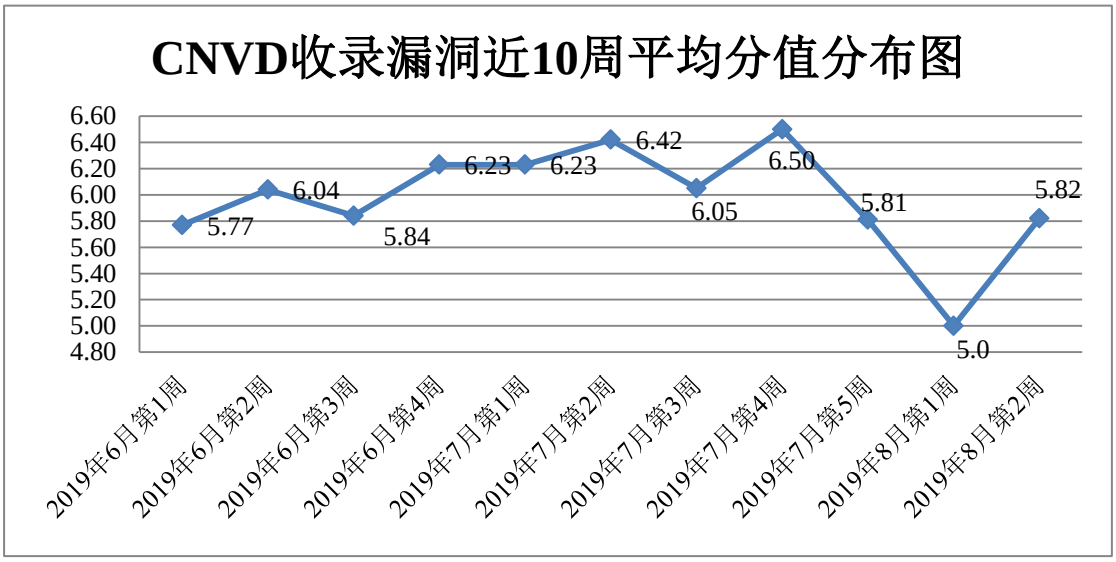

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 10 起，向银行、保险、能源等重要行业单位通报漏洞事件 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 217 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 11 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：

东莞市同享软件科技有限公司、优购科技有限公司、中国化学工程第七建设有限公司、北京正影网络科技有限公司、上海丹帆网络科技有限公司、中铁二十一局集团第三工程有限公司、煤炭科学技术研究院有限公司、淄博闪灵网络科技有限公司、江苏楚淮软件科技开发有限公司、淮南市银泰软件科技有限公司、拾联（厦门）信息科技有限公司、洪湖尔创网联信息技术有限公司、北京网康科技有限公司、广州合优网络科技有限公司、上海卓卓网络科技有限公司、北京康盛新创科技有限责任公司、山西先启科技有限公司、北京亚控科技发展有限公司、上海融励科技有限公司、重庆远秋科技公司、南京苏迪科技有限公司、长沙翱云网络科技有限公司、北京米尔伟业科技有限公司、Apowersoft 有限公司、中国钛锆铪协会、中国报道网、中国建筑出版在线、平凡软件、海洋 cms、信呼、TuziCMS、ZZCMS、PHPMywind 和 SoftMaker。

本周，CNVD 发布了《Microsoft 发布 2019 年 8 月安全更新》和《关于 Microsoft 远程桌面服务存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5163

https://www.cnvd.org.cn/webinfo/show/5165

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、华为技术有限公司、深信服科技股份有限公司、厦门服云信息科技有限公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、国瑞数码零点实验室、国网思极检测技术（北京）有限公司、山东新潮信息技术有限公司、北京铭图天成信息技术有限公司、上海银基信息安全技术股份有限公司、山东华鲁科技发展股份有限公司、内蒙古奥创科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、长春嘉诚信息技术股份有限公司、北京圣博润高新技术股份有限公司、广州锦行网络科技有限公司、成都久信信息技术股份有限公司、喵斯科技、北京智游网安科技有限公司、山石网科通信技术有限公司、广州非凡信息安全技术有限公司及其他个人白帽子向 CNVD 提交了 1469 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 845 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）	581	581
奇安信网神（补天平台）	264	264
北京天融信网络安全技术有限公司	237	18
哈尔滨安天科技集团股份有限公司	224	0
华为技术有限公司	206	0
深信服科技股份有限公司	175	0
厦门服云信息科技有限公司	58	0
新华三技术有限公司	55	0
北京启明星辰信息安全技术有限公司	49	0
北京神州绿盟科技有限公司	49	0
恒安嘉新(北京)科技股份公司	32	0
西安四叶草信息技术有限公司	22	22
中新网络信息安全股份有限公司	21	0
北京数字观星科技有限公司	21	0
中新网络信息安全股份有限公司	21	21
四川无声信息技术有限公司	17	17
南京联成科技发展股份有限公司	8	8
西门子（中国）有限公司	6	0
北京知道创宇信息技术股份有限公司	3	0
山东云天安全技术有限公司	80	80
国瑞数码零点实验室	52	52
国网思极检测技术（北京）有限公司	44	44

山东新潮信息技术有限公司	38	38
北京铭图天成信息技术有限公司	35	35
上海银基信息安全技术股份有限公司	27	27
山东华鲁科技发展股份有限公司	20	20
内蒙古奥创科技有限公司	14	14
远江盛邦（北京）网络安全科技股份有限公司	13	13
长春嘉诚信息技术股份有限公司	12	12
北京圣博润高新技术股份有限公司	9	9
广州锦行网络科技有限公司	6	6
成都久信信息技术股份有限公司	3	3
喵斯科技	3	3
北京智游网安科技有限公司	2	2
山石网科通信技术有限公司	2	2
广州非凡信息安全技术有限公司	1	1
CNCERT 西藏分中心	13	13
CNCERT 河北分中心	8	8
CNCERT 四川分中心	5	5
CNCERT 天津分中心	3	3
CNCERT 贵州分中心	2	2
CNCERT 黑龙江分中心	2	2
CNCERT 云南分中心	2	2
个人	142	142

报送总计	2587	1469

本周漏洞按类型和厂商统计

本周，CNVD 收录了 498 个漏洞。应用程序 268 个，WEB 应用 142 个，操作系统 44 个，数据库 13 个，智能设备（物联网终端设备）12 个，网络设备（交换机、路由器等网络端设备）11 个，安全产品 8 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	268
WEB 应用	142
操作系统	44
数据库	13
智能设备（物联网终端设备）	12
网络设备（交换机、路由器等网络端设备）	11
安全产品	8

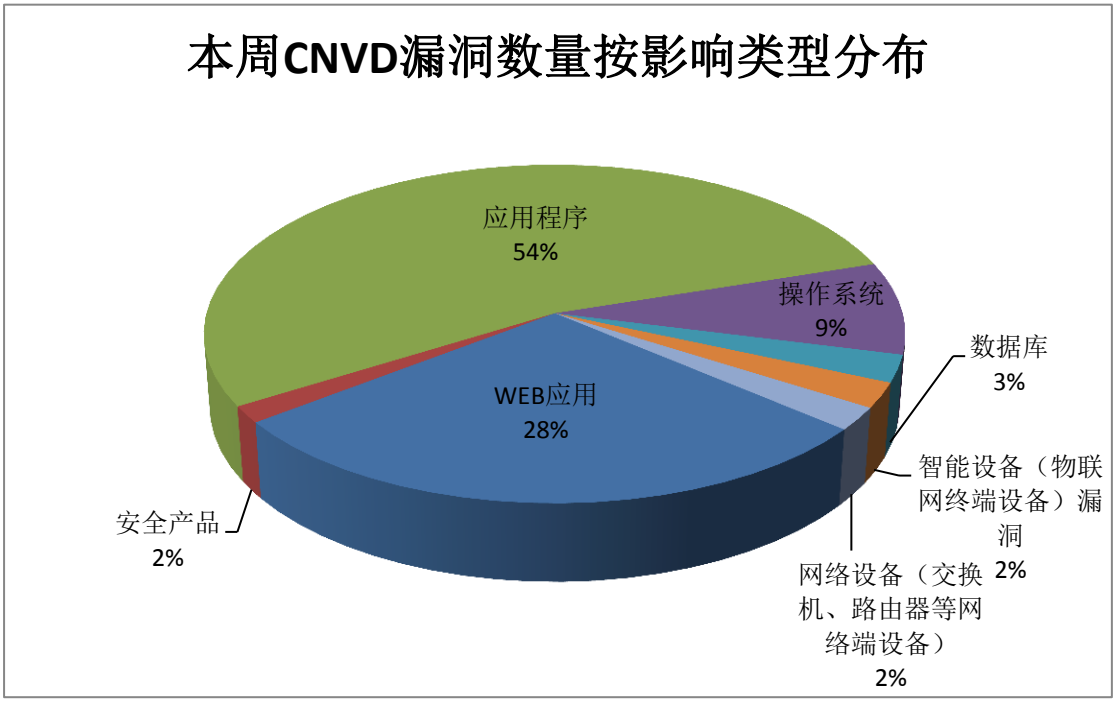

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、WordPress、cPanel 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	65	13%
2	WordPress	55	11%
3	Microsoft	46	9%
4	cPanel	35	7%
5	Adobe	22	5%
6	Google	20	4%
7	Jsish	8	2%
8	Amazon	7	1%
9	IBM	7	1%
10	其他	233	47%

本周行业漏洞收录情况

本周，CNVD 收录了 4 个电信行业漏洞，28 个移动互联网行业漏洞，9 个工控行业漏洞（如下图所示）。其中，“Cisco NX-OS Software 缓冲区溢出漏洞、PostgreSQL SQL 注入漏洞、Nextcloud Android app 代码注入漏洞、Google Android 缓冲区溢出漏洞（CNVD-2019-27589）”等漏洞的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，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/

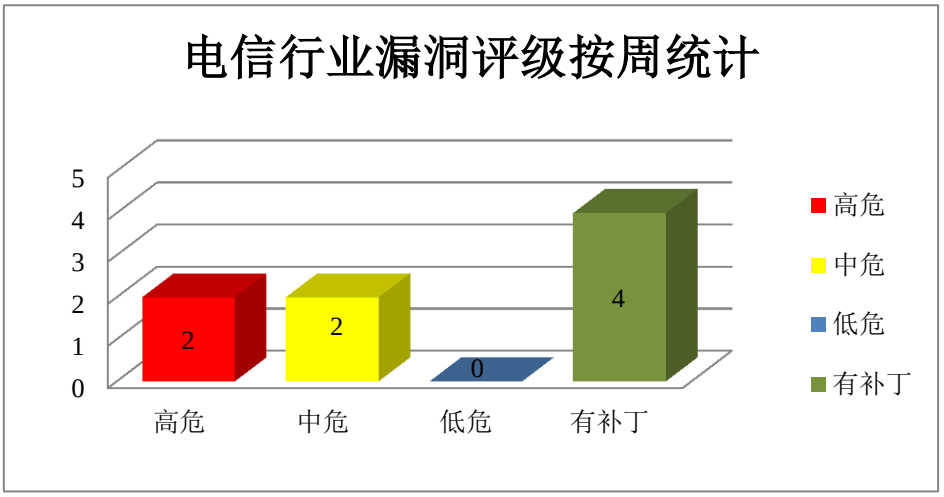

图 3 电信行业漏洞统计

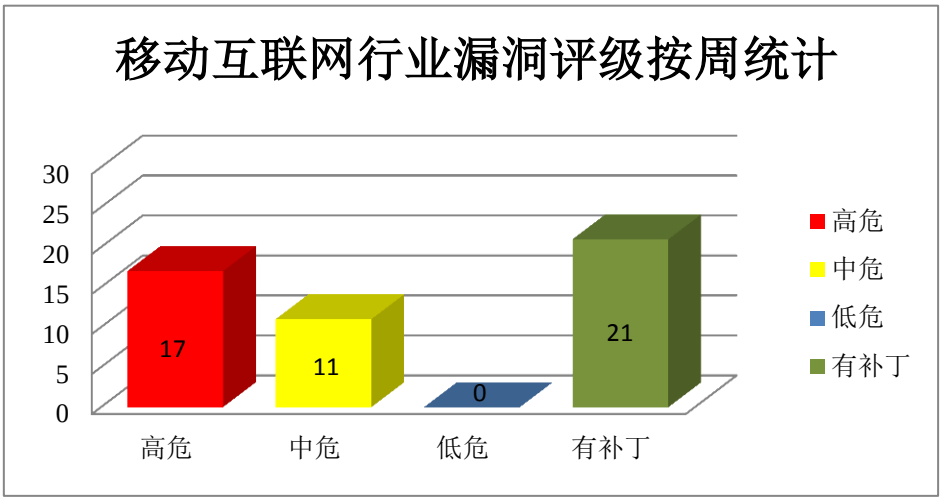

图 4 移动互联网行业漏洞统计

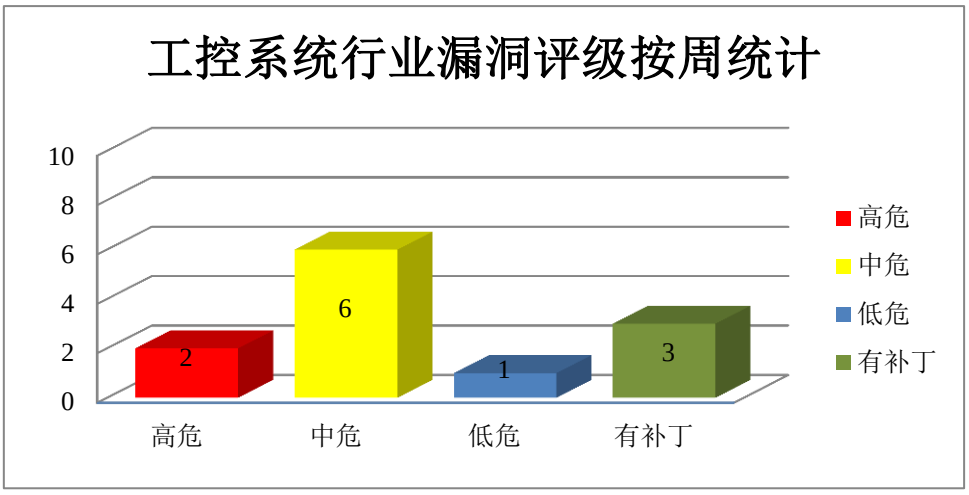

图 5 工控系统行业漏洞统计

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）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞执行代码。

CNVD 收录的相关漏洞包括：Google Android 缓冲区溢出漏洞（CNVD-2019-27574、CNVD-2019-27575、CNVD-2019-27576、CNVD-2019-27577、CNVD-2019-27579、CNVD-2019-27580、CNVD-2019-27578、CNVD-2019-27581）。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-2019-27574

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27575

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27576

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27577

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27579

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27580

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27578

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27581

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。Edge 是 Microsoft 公司为 Windows 10 打造的浏览器，特点是快速、安全。ChakraCore 是一个 Microsoft 开源的、用于 Windows IE/Edge 内核的高效 JS 脚本引擎。本周，该产品被披露存在内存破坏和远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Edge Chakra 脚本引擎内存破坏漏洞（CNVD-2019-27084、CNVD-2019-27085、CNVD-2019-27086、CNVD-2019-27087）、Microsoft Windows 远程桌面服务远程代码执行漏洞（CNVD-2019-27323、CNVD-2019-27324、CNVD-2019-27325、CNVD-2019-27325）。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-2019-27084

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27085

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27086

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27087

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27323

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27324

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27325

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27326

3、Adobe 产品安全漏洞

Adobe Photoshop，简称“PS”，是由 Adobe 公司开发和发行的图像处理软件。Photoshop CC 是 Photoshop Creative Cloud 版。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 Photoshop CC 越界写入漏洞（CNVD-2019-27490、CNVD-2019-27488、CNVD-2019-27489、CNVD-2019-27491、CNVD-2019-27492、CNVD-2019-27493、CNVD-2019-27494、CNVD-2019-27495）。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-2019-27490

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27488

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27489

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27491

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27492

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27493

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27494

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27495

4、Oracle 产品安全漏洞

Oracle Fusion Middleware（Oracle 融合中间件）是一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。WebLogic Server 是其中的一个适用于云环境和传统环境的应用服务器组件。Oracle Virtualization 是一套虚拟化解决方案。本周，上述产品被披露存在信息泄露和访问控制错误漏洞，攻击者可利用漏洞影响数据的保密性、完整性和可用性。

CNVD 收录的相关漏洞包括：Oracle WebLogic Server 组件信息泄露漏洞（CNVD-2019-27105、CNVD-2019-27106、CNVD-2019-27107、CNVD-2019-27108）、Oracle VM VirtualBox 访问控制错误漏洞（CNVD-2019-27293、CNVD-2019-27294、CNVD-2019-27296、CNVD-2019-27297）。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-2019-27105

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27106

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27107

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27108

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27293

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27294

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27296

http://www.cnvd.org.cn/flaw/show/CNVD-2019-27297

5、Edimax Wi-Fi Extender 跨站请求伪造漏洞

Edimax Technology Wi-Fi Extender 是一款无线信号扩展器。本周，Edimax Technology Wi-Fi Extender 被披露存在跨站请求伪造漏洞。攻击者可利用该漏洞通过受影响客户端向服务器发送非预期的请求。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-2019-26840

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-2019-26772	FreeBSD bhyve 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.freebsd.org/security/advisories/FreeBSD-SA-19:16.bhyve.asc
CNVD-2019-26799	Linaro OP-TEE 内存破坏漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/OP-TEE/optee_os/commit/e3adcf566cb278444830e7badfdcc3983e334fd1
CNVD-2019-26817	Slanger Message handler&request validator 命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/stevegraham/slanger/pull/238/commits/5267b455caeb2e055ccf0d2b6a22727c111f5c3
CNVD-2019-26823	AVTECH Software Room Alert 3E 权限提升漏洞	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://avtech.com/
CNVD-2019-26838	Apache Ranger 跨站请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger
CNVD-2019-27433	HPE 3PAR Service Processor 远程任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03942en_us
CNVD-2019-27436	OXID eSales OXID eShop SQL 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://oxidforge.org/en/security-bulletin-2019-001.html
CNVD-2019-27444	NVIDIA Windows GPU Display Driver DirectX 驱动缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.vmware.com/security/advisories/VMSA-2019-0012.html
CNVD-2019-27593	MailEnable 路径遍历漏洞	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.mailenable.com/Standard-ReleaseNotes.txt
CNVD-2019-27597	IBM Security Privileged Identity Manager 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：

			https://www-01.ibm.com/support/docview.wss?uid=ibm10879093

小结：本周，Google 被披露存在缓冲区溢出漏洞，攻击者可利用漏洞执行代码。此外，Microsoft、Adobe、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞影响数据的保密性、完整性和可用性。Edimax Wi-Fi Extender 被披露存在跨站请求伪造漏洞。攻击者可利用该漏洞通过受影响客户端向服务器发送非预期的请求。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、Aptana Jaxer wikilite 源码浏览器本地文件包含漏洞

验证描述

Aptana Jaxer 是一款开源的 JavaScript 服务器。

Aptana Jaxer 1.0.3.4547 版本中的 wikilite 源码浏览器存在本地文件包含漏洞。远程攻击者可借助 tools/sourceViewer/index.html?filename=../ URI 利用该漏洞读取内部文件。

验证信息

POC 链接：https://packetstormsecurity.com/files/153985/Aptana-Jaxer-1.0.3.4547-Local-File-Inclusion.html

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-26776

信息提供者

恒安嘉新(北京)科技股份公司

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. “螺丝刀”揭开严重安全漏洞，多厂商驱动程序及固件现提权问题

某网络安全研究公司公布了一份报告，称超过 20 家公司都会收到其发现的名为“螺丝刀”漏洞的影响。报告中，该公司称驱动程序及固件的不安全问题非常普遍，包括华硕、华擎等主要的 BIOS 供应商及 NVIDIA 等的驱动程序中都发现了严重漏洞，而且更严重的是他们发现的易受攻击的驱动程序都经过了微软的认证，因此他们已经邀请微软提供包括将一直的问题驱动列入黑名单等方法防范此类漏洞。这些漏洞都允许驱动程序充当代理，以执行对硬件资源的高权限访问，例如对处理器和芯片组的 I/O 空间的读写访问等。这是一种权限提升，因为它可以将攻击者从用户模式（Ring 3）提权至操作系

统的内核模式（Ring 0），这样恶意软件就会拥有更多的权限执行。而驱动程序中的漏洞会使恶意软件较为轻松的获取高等级权限。

参考链接：https://eclypsium.com/2019/08/10/screwed-drivers-signed-sealed-delivered/

2. Steam 被曝出 0day 提权漏洞

近期，全球流行的 Steam 游戏客户端被曝出 0day 提权漏洞，影响全球一亿多 Steam 用户。该漏洞可让机器上的低权限用户以 SYSTEM 权限运行程序。这意味着恶意软件很可能利用这个漏洞对受害者的机器进行深度破坏。

参考链接：https://nosec.org/home/detail/2847.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