国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 06 月 03 日-2019 年 06 月 09 日 **2019 年第 23 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 171 个，其中高危漏洞 54 个、中危漏洞 103 个、低危漏洞 14 个。漏洞平均分值为 5.77。本周收录的漏洞中，涉及 0day 漏洞 36 个（占 21%），其中互联网上出现“WordPress 插件 Ad-Manager 开放重定向漏洞、EmpireCMS 跨站脚本漏洞”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 1752 个，与上周（1605 个）环比增长 9%。

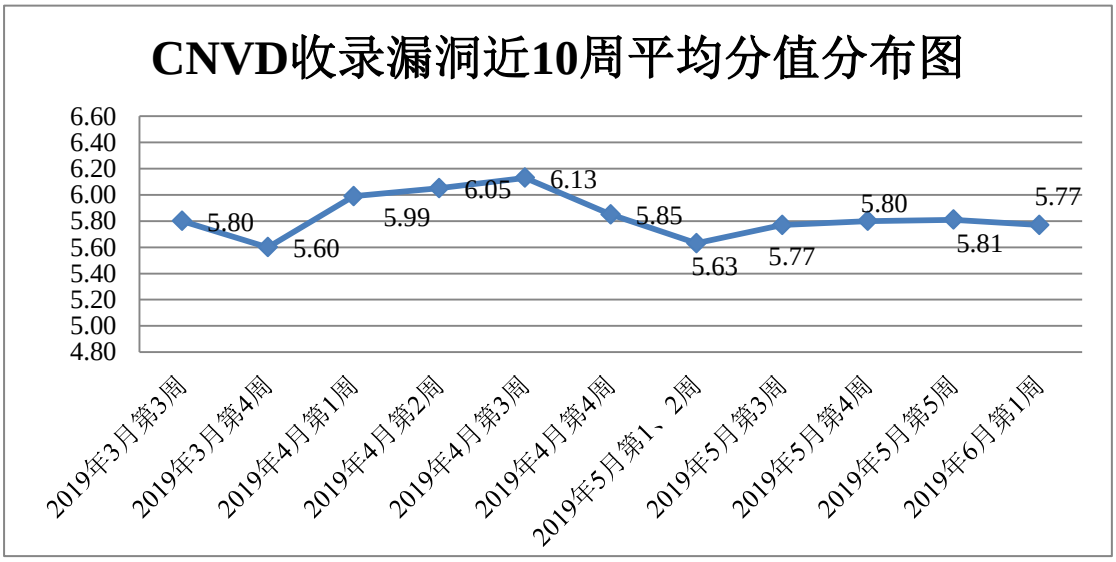

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 6 起，向银行、保险、能源等重要行业单位通报漏洞事件 11 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 263 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 7 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 7 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：

上海安达通信息安全技术股份有限公司、北京希遇信息科技有限公司、成都鹏博士电信传媒集团股份有限公司、西安至成信息科技有限公司、沧州市凡诺广告传媒有限公司、合肥拓野网络科技有限公司、上海亿速网络科技有限公司、深圳市前海中昊科技有限公司、中航善达股份有限公司、洛阳市恒凯信息科技有限公司、中铁二局贵阳驾驶培训有限公司、苏州托普斯网络科技有限公司、淄博闪灵网络科技有限公司、嘉兴想天信息科技有限公司、厦门易商网络科技有限公司、永康市中基互联科技有限公司、成都远成伟业信息技术有限公司、苏州天宫信息技术有限公司、浙江齐治科技股份有限公司、北京金航联科技发展有限公司、宿迁鑫潮信息技术有限公司、云南若水网络科技有限公司、北京二六三企业通信有限公司、中国电力企业联合会、中铁物流网、中国电子科技集团有限公司第二十二研究所、中国建筑钢结构网、爱客 CMS、施耐德（Schneider Electric）、苹果 CMS、苏州苏博科水环境保护科学研究院、中国知网。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，华为技术有限公司、哈尔滨安天科技集团股份有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、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。山东云天安全技术有限公司、任子行网络技术股份有限公司、南京众智维信息科技有限公司、内蒙古奥创科技有限公司、北京铭图天成信息技术有限公司、国瑞数码零点实验室、山东华鲁科技发展股份有限公司、上海并擎软件科技有限公司、河南信安世纪科技有限公司、北京圣博润高新技术股份有限公司、广州昊达信息科技有限公司、山石网科通信技术有限公司、北京君信安科技有限公司、江苏安又恒信息科技有限公司、上海物盾信息科技有限公司、浙江鹏信信息科技股份有限公司及其他个人白帽子向 CNVD 提交了 2163 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 1752 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）	1499	1499
奇安信网神（补天平台）	253	253
华为技术有限公司	199	0

哈尔滨安天科技集团股份有限公司	85	0
北京天融信网络安全技术有限公司	73	2
新华三技术有限公司	69	3
北京启明星辰信息安全技术有限公司	48	4
深信服科技股份有限公司	45	0
北京神州绿盟科技有限公司	32	0
中国电信集团系统集成有限责任公司	31	0
西安四叶草信息技术有限公司	14	14
中新网络信息安全股份有限公司	14	14
恒安嘉新(北京)科技股份公司	13	1
北京数字观星科技有限公司	11	0
南京联成科技发展股份有限公司	8	8
北京知道创宇信息技术股份有限公司	3	0
杭州安恒信息技术股份有限公司	2	2
山东云天安全技术有限公司	38	38
任子行网络技术股份有限公司	36	36
南京众智维信息科技有限公司	35	35
内蒙古奥创科技有限公司	28	28
北京铭图天成信息技术有限公司	22	22
国瑞数码零点实验室	13	13
山东华鲁科技发展股份有限公司	8	8
上海并擎软件科技有限公司	8	8

河南信安世纪科技有限公司	3	3
北京圣博润高新技术股份有限公司	2	2
广州昊达信息科技有限公司	2	2
山石网科通信技术有限公司	1	1
北京君信安科技有限公司	1	1
江苏安又恒信息科技有限公司	1	1
上海物盾信息科技有限公司	1	1
浙江鹏信信息科技股份有限公司	1	1
CNCERT 甘肃分中心	6	6
CNCERT 海南分中心	2	2
CNCERT 贵州分中心	1	1
个人	154	154
报送总计	2762	2163

本周漏洞按类型和厂商统计

本周，CNVD 收录了 171 个漏洞。应用程序 98 个，操作系统 27 个，WEB 应用 26 个，网络设备（交换机、路由器等网络端设备）9 个，数据库 8 个，安全产品 2 个，智能设备（物联网终端设备）漏洞 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	98
操作系统	27
WEB 应用	26
网络设备（交换机、路由器等网络端设备）	9
数据库	8
安全产品	2
智能设备（物联网终端设备）漏洞	1

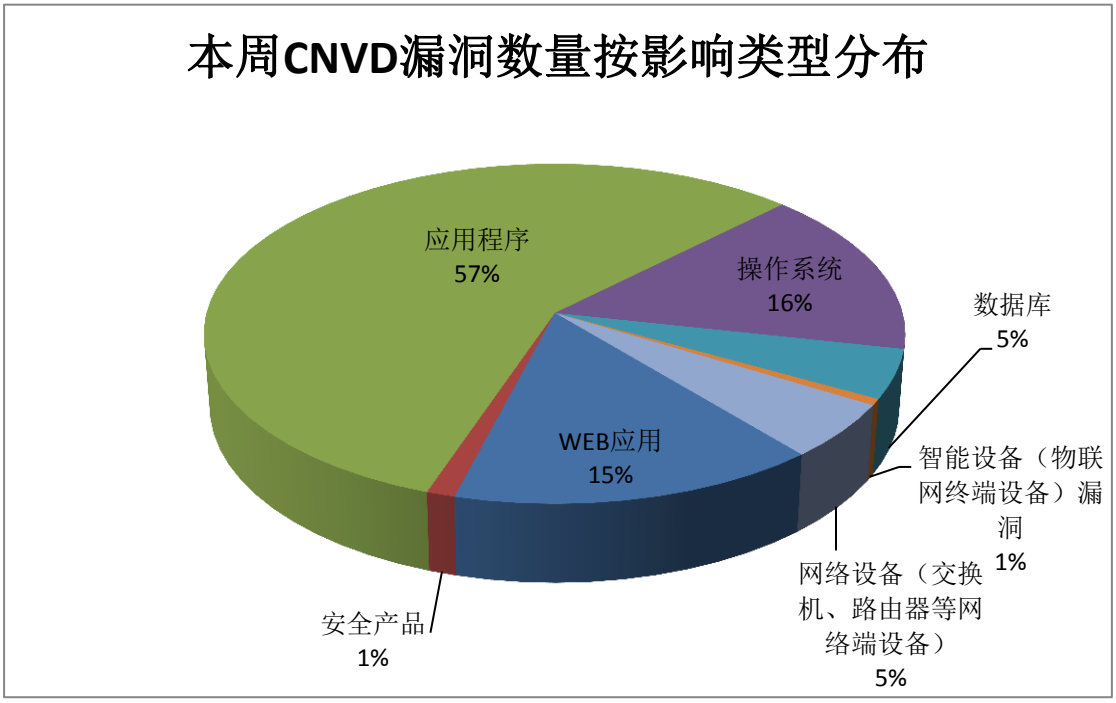

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Adobe、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	Microsoft	22	13%
2	Adobe	13	8%
3	Oracle	11	6%
4	PHP Scripts Mall	9	5%
5	Linux	8	5%
6	Computrols	7	4%
7	WordPress	5	3%
8	NTPsec	4	2%
9	Apple	3	2%
10	其他	89	52%

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，5 个移动互联网行业漏洞（如下图所示）。其中，“PostgreSQL 代码执行漏洞（CNVD-2019-16483）、Oracle Database Server Core RDBMS 访问控制错误漏洞、多款 Apple 产品 WebKit 组件缓冲区溢出漏洞、Oracle Dat

abase Server Java VM 访问控制错误漏洞”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/

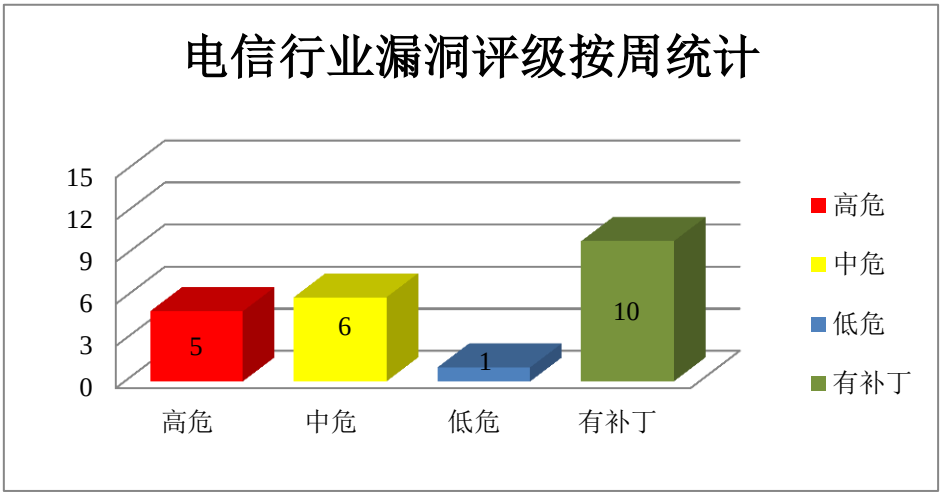

图 3 电信行业漏洞统计

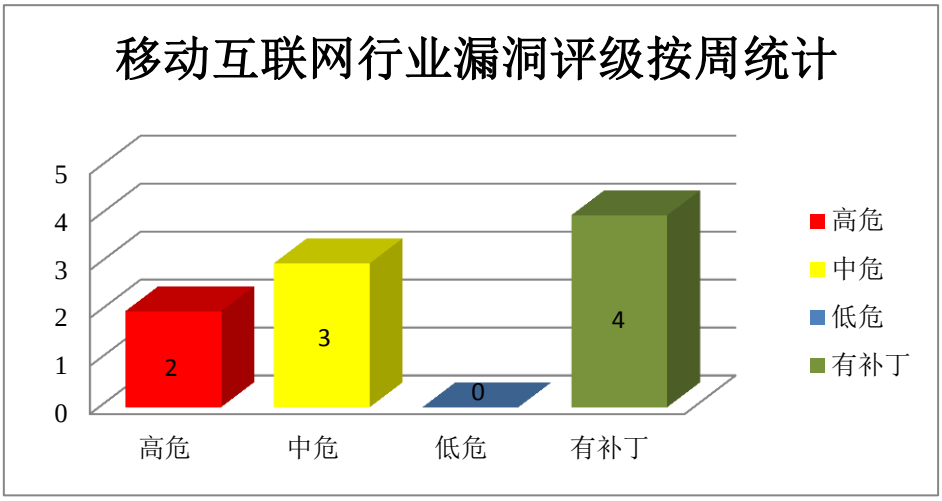

图 4 移动互联网行业漏洞统计

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多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 信息泄露漏洞（CNVD-2019-16540）、Adobe Acrobat 和 Reader 堆溢出漏洞（CNVD-2019-16536、CNVD-2019-165

35）、Adobe Acrobat 和 Reader 类型混淆漏洞（CNVD-2019-16538、CNVD-2019-16537、CNVD-2019-16539）、Adobe Acrobat 和 Reader 越界读取漏洞（CNVD-2019-16541、CNVD-2019-16542）。其中，除“Adobe Acrobat 和 Reader 越界读取漏洞（CNVD-2019-16541、CNVD-2019-16542）”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：http://www.cnvd.org.cn/flaw/show/CNV-2019-16540

http://www.cnvd.org.cn/flaw/show/CNV-2019-16536

http://www.cnvd.org.cn/flaw/show/CNV-2019-16535

http://www.cnvd.org.cn/flaw/show/CNV-2019-16538

http://www.cnvd.org.cn/flaw/show/CNV-2019-16537

http://www.cnvd.org.cn/flaw/show/CNV-2019-16539

http://www.cnvd.org.cn/flaw/show/CNV-2019-16541

http://www.cnvd.org.cn/flaw/show/CNV-2019-16542

2、Oracle 产品安全漏洞

Oracle E-Business Suite（电子商务套件）是一套全面集成式的全球业务管理软件。Oracle Database Server 是一套关系数据库管理系统。Oracle MySQL 是一套开源的关系数据库管理系统。Oracle Retail Applications 是一套零售应用商店解决方案。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 E-Business Suite One-to-One Fulfillment 访问控制错误漏洞、Oracle Database Server Core RDBMS 访问控制错误漏洞、Oracle Database Server Java VM 访问控制错误漏洞、Oracle MySQL Server 访问控制错误漏洞（CNVD-2019-16278、CNVD-2019-16397）、Oracle Retail Applications Retail Convenience Store Back Office 访问控制错误漏洞、Oracle Retail Applications MICROS Relate CRM Software 访问控制错误漏洞、Oracle Retail Applications MICROS Lucas 访问控制错误漏洞。其中，“Oracle E-Business Suite One-to-One Fulfillment 访问控制错误漏洞、Oracle Database Server Core RDBMS 访问控制错误漏洞、Oracle Database Server Java VM 访问控制错误漏洞、Oracle Retail Applications Retail Convenience Store Back Office 访问控制错误漏洞”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-2019-16274

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16276

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16275

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16278

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16397

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16395

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16398

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16399

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。Windows Graphics Device Interface（GDI）是其中的一个图形设备接口。Microsoft 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。本周，上述产品被披露存在缓冲区溢出和远程代码执行漏洞，攻击者可利用漏洞执行任意代码，造成内存破坏。

CNVD 收录的相关漏洞包括：Microsoft Edge 和 ChakraCore 缓冲区溢出漏洞（CNVD-2019-16511）、Microsoft Windows GDI 远程代码执行漏洞（CNVD-2019-16510）、Microsoft ChakraCore 和 Microsoft Edge 远程代码执行漏洞（CNVD-2019-16745、CNVD-2019-16746、CNVD-2019-16748）、Microsoft Edge 远程代码执行漏洞（CNVD-2019-16747）、Microsoft Edge 和 ChakraCore 远程代码执行漏洞（CNVD-2019-16749）、多款 Microsoft 产品远程代码执行漏洞（CNVD-2019-16750）。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-2019-16511

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16510

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16745

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16746

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16747

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16749

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16748

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16750

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞获取网站管理员访问权限，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Linux kernel 输入验证错误漏洞、Linux kernel 内存泄露漏洞、Linux kernel 内存分配失败处理不当漏洞、Linux kernel 拒绝服务漏洞（CNVD-2019-16431、CNVD-2019-16432、CNVD-2019-16590、CNVD-2019-16599、CNVD-2019-16428）。其中，“Linux kernel 输入验证错误漏洞、Linux kernel 拒绝服务漏洞（CNVD-2019-16590、CNVD-2019-16599）” 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-2019-16402
http://www.cnvd.org.cn/flaw/show/CNVD-2019-16429
http://www.cnvd.org.cn/flaw/show/CNVD-2019-16430
http://www.cnvd.org.cn/flaw/show/CNVD-2019-16431
http://www.cnvd.org.cn/flaw/show/CNVD-2019-16432
http://www.cnvd.org.cn/flaw/show/CNVD-2019-16590
http://www.cnvd.org.cn/flaw/show/CNVD-2019-16599
http://www.cnvd.org.cn/flaw/show/CNVD-2019-16428

5、Samsung SCX-824 跨站脚本漏洞

Samsung SCX-824 是一款多功能打印机。

Samsung SCX-824 被披露存在跨站脚本漏洞。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。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-2019-16420

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-2019-16270	Computrols CBAS Web 命令注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://www.computrols.com/support/technical-support/
CNVD-2019-16272	Docker API 端点路径遍历漏洞	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.docker.com/
CNVD-2019-16415	Facebook WhatsApp 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.facebook.com/security/advisories/cve-2019-3568
CNVD-2019-16416	IBM i2 Intelligent Analyis Platform XML 外部实体漏洞	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=ibm10881746
CNVD-2019-16421	OIC Exponent CMS SQL 注入漏洞（CNVD-2019-16421）	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/exponentcms/expone

			nt-cms/commit/99636b2118cd9af4eb9920f6b6c228bd824593d
CNVD-2019-16481	Serendipity 代码注入漏洞	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/s9y/Serendipity/releases/tag/2.0.4
CNVD-2019-16527	Mitsubishi Electric MELSEC-Q Series PLCs 远程拒绝服务漏洞	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.mitsubishielectric.com/
CNVD-2019-16526	Exponent CMS 对象注入漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://github.com/exponentcms/exponent-cms/commit/fdafb5ec97838e4edbd685f587f28d3174ebb3db
CNVD-2019-16532	OIC Exponent CMS SQL 注入漏洞（CNVD-2019-16532）	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/exponentcms/exponent-cms/commit/fdafb5ec97838e4edbd685f587f28d3174ebb3db
CNVD-2019-16580	HP Workstation BIOS 代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://support.hp.com/us-en/document/c06318199

小结：本周，Adobe 被披露存在缓冲区溢出漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码。此外，Oracle、Microsoft、Linux 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取网站管理员访问权限，执行任意代码，造成内存破坏等。Samsung SCX-824 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、WordPress 插件 Ad-Manager 开放重定向漏洞

验证描述

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。

WordPress 插件 Ad-Manager 存在开放重定向漏洞。攻击者可成功启动网络钓鱼欺诈，并且窃取用户凭据。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=33204

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-16597

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. 全新的 RCE 漏洞影响了近一半电子邮件服务器

近日，安全研究人员透露，一个关键的远程命令执行（RCE）安全漏洞影响了超过一半的互联网电子邮件服务器。该漏洞影响 Exim，一种邮件传输代理（MTA）服务，用于将电子邮件从发件人中继到收件人。根据 2019 年 6 月对互联网上可见的所有邮件服务器的调查，57%（507,389）的电子邮件服务器运行 Exim 服务，还有报告称实际数量为该数字的 10 倍，即 540 万。该漏洞允许本地或远程攻击者以 root 用户身份在 Exim 服务器上运行命令并接管系统。在发给 Linux 发行版维护者的电子邮件中，Qualys 表示该漏洞“非常容易被利用”，并预计攻击者会在未来几天内提出漏洞利用代码。

参考链接：https://www.zdnet.com/article/new-rce-vulnerability-impacts-nearly-half-of-the-internets-email-servers/#ftag=RSSbaffb68

2. 黑客可劫持远程桌面会话，绕过 Windows 锁屏

卡耐基梅隆大学的 CERT 协调中心近日发布预警称， Windows 远程桌面服务的网络级身份验证（NLA）功能可被黑客利用，绕过 Windows 的锁屏。黑客主要是通过 0-day 漏洞（CVE-2019-9510）劫持现有的远程桌面服务会话，绕过锁屏并获取对计算机的访问权限。即使计算机开启双因素认证也无济于事。这个漏洞主要影响 Windows 1803 之后的 Windows 10 版本，以及 Server 2019 或更新版本。目前，微软尚未发布相关补丁。

参考链接：https://www.securityweek.com/hackers-can-bypass-windows-lockscreen-remote-desktop-sessions

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