国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 10 月 14 日-2019 年 10 月 20 日 **2019 年第 42 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 406 个，其中高危漏洞 100 个、中危漏洞 270 个、低危漏洞 36 个。漏洞平均分值为 5.60。本周收录的漏洞中，涉及 0day 漏洞 84 个（占 21%），其中互联网上出现“WordPress ACF-Frontend-Display 插件文件上传漏洞、Libntlm 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 3527 个，与上周（4763 个）环比减少 25%。

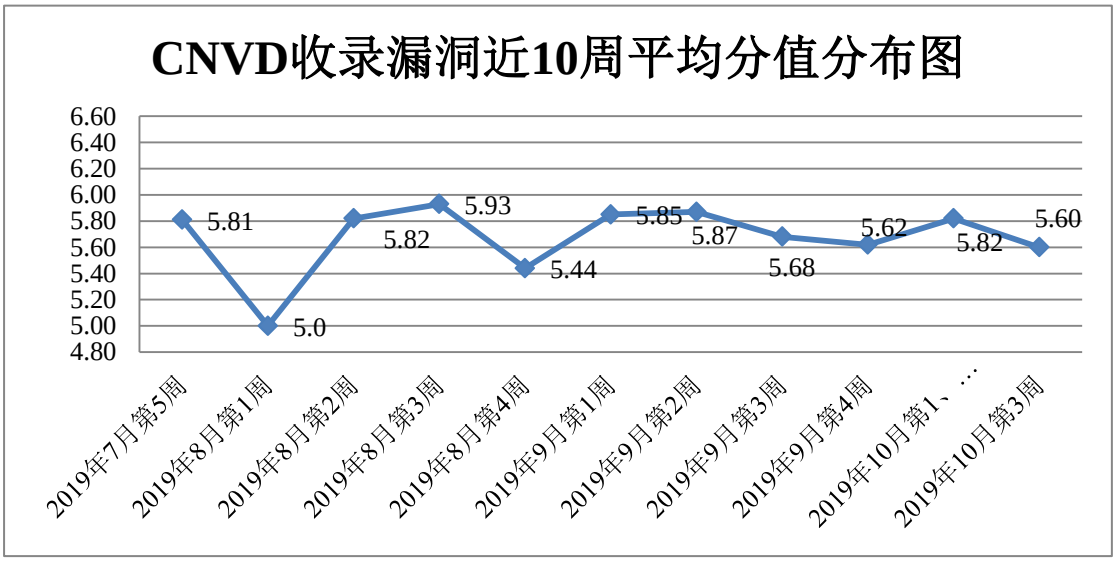

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 1 起，向银行、保险、能源等重要行业单位通报漏洞事件 50 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 366 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 55 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25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：

虎扑（上海）文化传播股份有限公司、北京陌陌科技有限公司、北京京东世纪贸易有限公司、广州酷狗计算机科技有限公司、乐视控股(北京)有限公司、北京墨迹风云科技股份有限公司、网易公司、北京良精志诚科技有限责任公司、杭州帕拉迪网络科技有限公司、淮南市银泰软件科技有限公司、帆软软件有限公司、江苏极元信息技术有限公司、格林豪泰酒店（中国）有限公司、上海端御信息科技有限公司、上海泛微网络科技股份有限公司、广州瀚德网络科技有限公司、苏州浩辰软件股份有限公司、悦阁网络科技有限公司、深圳昆仑通态科技有限责任公司、宿迁市展鸿网络科技有限公司、杭州联创信息技术有限公司、南京品德科技有限责任公司、上海三盟软件有限公司、成都火狐狸科技有限公司、广州恒企教育科技有限公司、北京华宇信息技术有限公司、北京正影网络科技有限公司、海南赞赞网络科技有限公司、深圳市云房网络科技有限公司、上海大智慧股份有限公司、北京畅行信息技术有限公司、北京豆网科技有限公司、国美在线电子商务有限公司、北京密境和风科技有限公司、深圳市锟铻科技有限公司、哈尔滨伟成科技有限公司、北京贞观雨科技有限公司、北京一点网聚科技有限公司、百胜餐饮集团有限公司、上海寻梦信息技术有限公司、北京学而思教育科技有限公司、中国化学工程第十三建设有限公司、淄博闪灵网络科技有限公司、北京小米科技有限责任公司、北京卓易讯畅科技有限公司、北京淘友天下科技发展有限公司、暴风集团股份有限公司、优慕课在线教育科技（北京）有限责任公司、西安佰联网络技术有限公司、深圳市龙艺脉网络科技有限公司、帝兴软件开发有限公司、苏宁安全应急响应中心、OPPO安全应急响应中心、美团安全应急响应中心、中国组织化学与细胞化学杂志、深圳龙脉科技、当当网、中国化工学会、UQCMS、Tencent WeGame、Xnview、SemCms、SeaCMS、Oracle、ROCK IN MUSIC、CheerWeb、Guojiz 和 SchoolCMS。

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、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、北京神州绿盟科技有限公司、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。远江盛邦（北京）网络安全科技股份有限公司、国瑞数码零点实验室、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、山东云天安全技术有限公司、北京铭图天成信息技术有限公司、南京众智维信息科技有限公司、上海并擎软件科技有限公司、内蒙古奥创科技有限公司、北京君信安科技有限公司、山东华鲁科技发展股份有限公司、北京智游网安科技有限公司、上海端御信息科技有限公司、杭州美创科技有限公司、北京圣博润高新技术股份有限公司、

弘康人寿保险股份有限公司、兰州冠云科技发展有限公司、山石网科通信技术股份有限公司及其他个人白帽子向 CNVD 提交了 3551 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 2763 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）	1299	1299
斗象科技（漏洞盒子）	956	956
上海交大	508	508
华为技术有限公司	283	0
北京天融信网络安全技术有限公司	220	1
哈尔滨安天科技集团股份有限公司	202	0
北京神州绿盟科技有限公司	104	5
深信服科技股份有限公司	61	0
新华三技术有限公司	60	0
厦门服云信息科技有限公司	29	0
北京数字观星科技有限公司	23	0
恒安嘉新(北京)科技股份公司	20	0
北京知道创宇信息技术股份有限公司	7	1
四川无声信息技术有限公司	67	67
中国电信集团系统集成有限责任公司	96	96
中新网络信息安全股份有限公司	20	20
远江盛邦（北京）网络安全科技股份有限公司	104	104
国瑞数码零点实验室	97	97

长春嘉诚信息技术股份有限公司	89	89
山东新潮信息技术有限公司	51	51
山东云天安全技术有限公司	35	35
北京铭图天成信息技术有限公司	26	26
南京众智维信息科技有限公司	25	25
上海并擎软件科技有限公司	12	12
内蒙古奥创科技有限公司	9	9
北京君信安科技有限公司	8	8
山东华鲁科技发展股份有限公司	4	4
北京智游网安科技有限公司	2	2
上海端御信息科技有限公司	2	2
杭州美创科技有限公司	1	1
北京圣博润高新技术股份有限公司	1	1
弘康人寿保险股份有限公司	1	1
兰州冠云科技发展有限公司	1	1
山石网科通信技术股份有限公司	1	1
CNCERT 浙江分中心	2	2
CNCERT 黑龙江分中心	1	1
个人	126	126
报送总计	4553	3551

本周漏洞按类型和厂商统计

本周，CNVD 收录了 406 个漏洞。应用程序 273 个，WEB 应用 79 个，操作系统 3

7 个，智能设备（物联网终端设备）11 个，网络设备（交换机、路由器等网络端设备）5 个，安全产品 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	273
WEB 应用	79
操作系统	37
智能设备（物联网终端设备）	11
网络设备（交换机、路由器等网络端设备）	5
安全产品	1

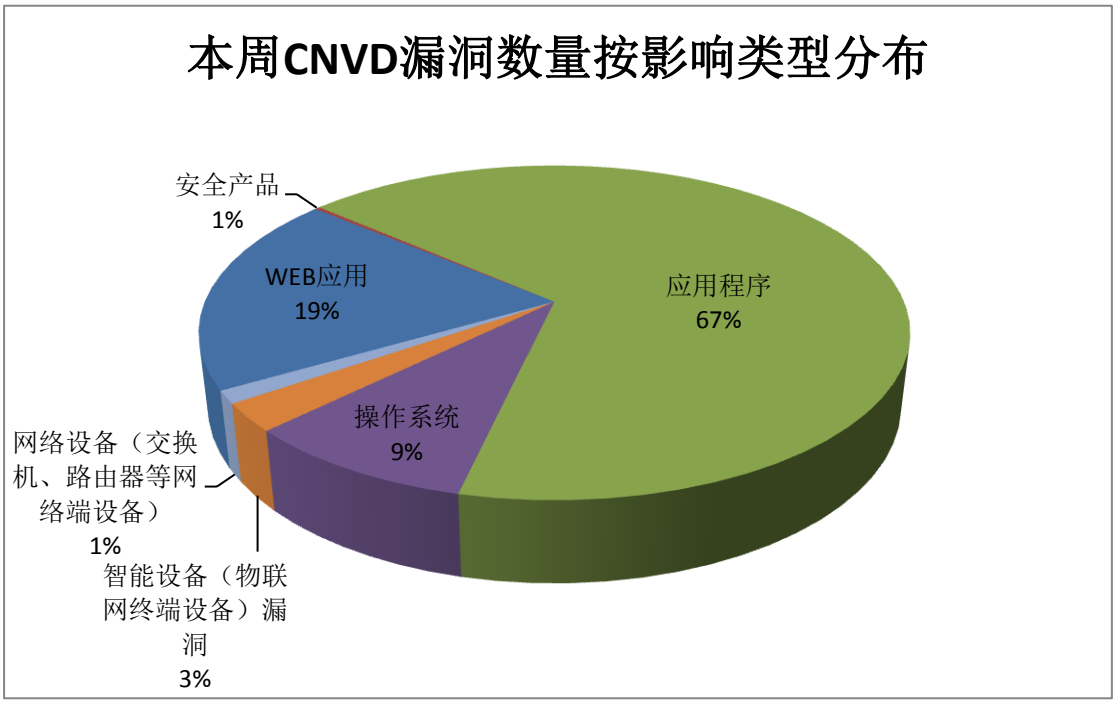

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、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	Adobe	68	17%
2	WordPress	66	16%
3	cPanel	42	10%
4	Google	35	9%
5	CloudBees	35	9%
6	Oracle	34	8%

7	Moodle	17	4%
8	Microsoft	11	3%
9	Atlassian	7	2%
10	其他	91	22%

本周行业漏洞收录情况

本周，CNVD 收录了 4 个电信行业漏洞，32 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“Electric Sheep Fencing pfsense 命令注入漏洞、Apple macOS、iCloud for Windows 和 iTunes for Windows UIFoundation 组件缓冲区溢出漏洞”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/

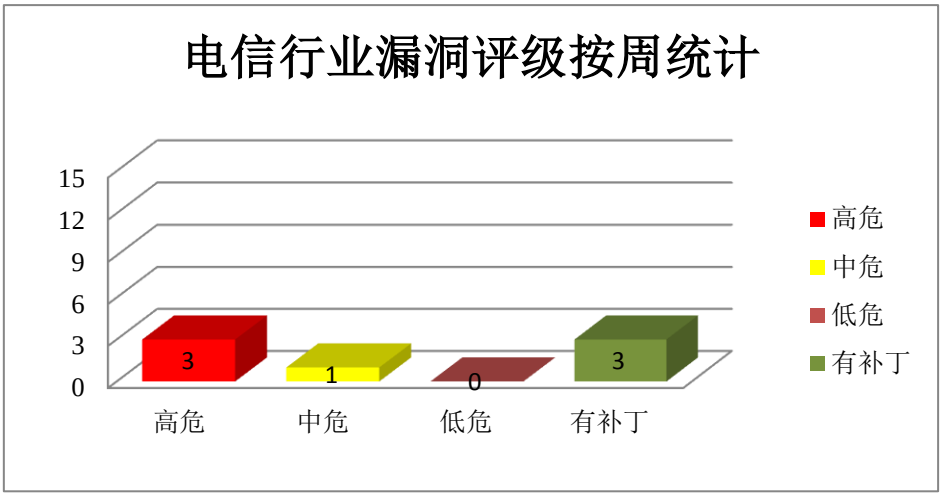

图 3 电信行业漏洞统计

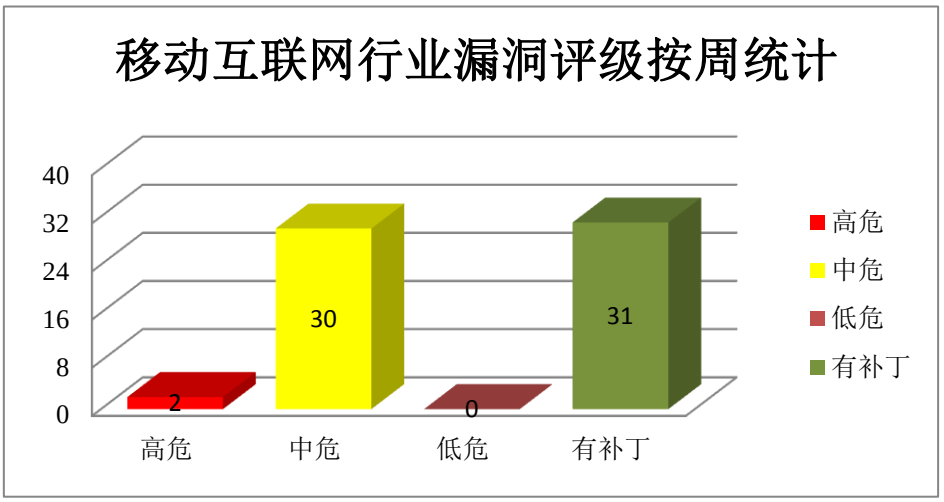

图 4 移动互联网行业漏洞统计

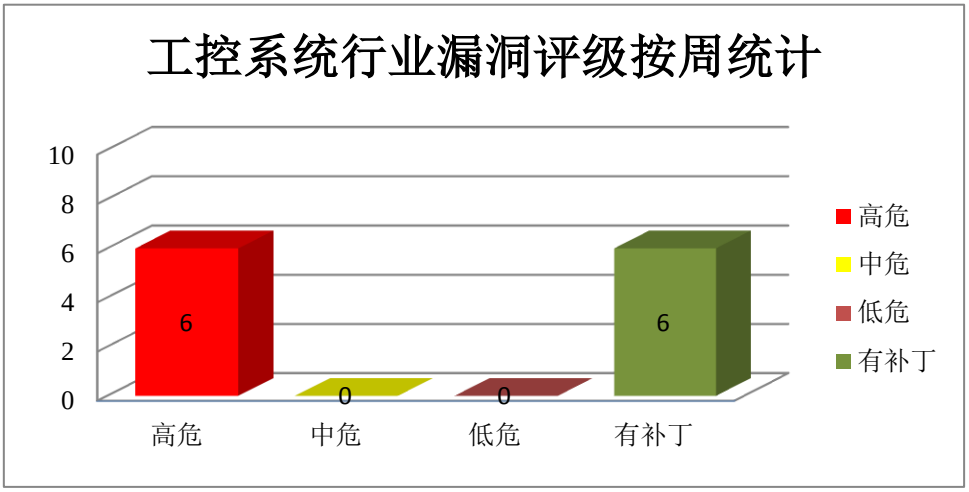

图 5 工控系统行业漏洞统计

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 Acrobat 是由 Adobe 公司开发的一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是 Adobe 公司开发的一款 PDF 文件阅读软件。本周，该产品被披露存在内存错误引用漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Acrobat/Reader 内存错误引用漏洞（CNVD-2019-35604、CNVD-2019-35605、CNVD-2019-35606、CNVD-2019-35607、CNVD-2019-35608、CNVD-2019-35610、CNVD-2019-35611、CNVD-2019-35609）。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-2019-35604

http://www.cnvd.org.cn/flaw/show/CNVD-2019-35605

http://www.cnvd.org.cn/flaw/show/CNVD-2019-35606

http://www.cnvd.org.cn/flaw/show/CNVD-2019-35607

http://www.cnvd.org.cn/flaw/show/CNVD-2019-35608

http://www.cnvd.org.cn/flaw/show/CNVD-2019-35610

http://www.cnvd.org.cn/flaw/show/CNVD-2019-35611

http://www.cnvd.org.cn/flaw/show/CNVD-2019-35609

2、Microsoft 产品安全漏洞

Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。Microsoft SharePoint 是一套企业业务协作平台。Microsoft Edge 是一款 Windows 10 之后

版本系统附带的 Web 浏览器。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 Dynamics 365 是一套适用于跨国企业的 ERP 业务解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，获取信息，造成内存损坏等。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2019-35567、CNVD-2019-35571）、Microsoft SharePoint 跨站脚本漏洞（CNVD-2019-35572）、Microsoft Internet Explorer 和 Microsoft Edge 欺骗漏洞、Microsoft Graphics 组件信息泄露漏洞、Microsoft Dynamics 365 跨站脚本漏洞（CNVD-2019-35573）、Microsoft Windows Hyper-V 信息泄露漏洞（CNVD-2019-35574）、Microsoft Internet Explorer 缓冲区溢出漏洞（CNVD-2019-35806）。其中，“Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2019-35567、CNVD-2019-35571）、Microsoft Internet Explorer 缓冲区溢出漏洞（CNVD-2019-35806）”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-2019-35567
http://www.cnvd.org.cn/flaw/show/CNVD-2019-35571
http://www.cnvd.org.cn/flaw/show/CNVD-2019-35572
http://www.cnvd.org.cn/flaw/show/CNVD-2019-35575
http://www.cnvd.org.cn/flaw/show/CNVD-2019-35576
http://www.cnvd.org.cn/flaw/show/CNVD-2019-35573
http://www.cnvd.org.cn/flaw/show/CNVD-2019-35574
http://www.cnvd.org.cn/flaw/show/CNVD-2019-35806

3、WordPress 产品安全漏洞

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。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，执行非法 SQLmingl，修改网络系统或组件的预期的执行控制流等。

CNVD 收录的相关漏洞包括：WordPress LifterLMS 插件提权漏洞、WordPress wp-editor 插件权限许可和访问控制问题漏洞、WordPress new-contact-form-widget 插件 SQL 注入漏洞、WordPress wti-like-post 插件 SQL 注入漏洞、WordPress liveforms 插件跨站脚本漏洞、WordPress events-manager 插件代码注入漏洞、WordPress liveforms 插件 SQL 注入漏洞、WordPress broken-link-manager 插件 SQL 注入漏洞。其中，除“WordPress liveforms 插件跨站脚本漏洞”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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-35217

http://www.cnvd.org.cn/flaw/show/CNVD-2019-35219

http://www.cnvd.org.cn/flaw/show/CNVD-2019-35883

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36053

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36075

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36079

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36083

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36207

4、cPanel 产品安全漏洞

cPanel 是美国 cPanel 公司的一套基于 Web 的自动化主机托管平台。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私人邮件，执行任意代码，进行任意文件名和文件 chmod 操作等。

CNVD 收录的相关漏洞包括：cPanel 输入验证错误漏洞（CNVD-2019-36129、CNVD-2019-36128、CNVD-2019-36133、CNVD-2019-36132、CNVD-2019-36131、CNVD-2019-36136）、cPanel 授权问题漏洞（CNVD-2019-36140）、cPanel 代码问题漏洞。其中，“cPanel 输入验证错误漏洞（CNVD-2019-36136）、cPanel 授权问题漏洞（CNVD-2019-36140）、cPanel 代码问题漏洞”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-2019-36129

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36128

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36133

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36132

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36131

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36136

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36140

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36147

5、Foxit PhantomPDF Dwg2Pdf DXF 文件解析内存破坏远程代码执行漏洞

Foxit PhantomPDF 是中国福昕（Foxit）公司的一款 PDF 文档阅读器。本周，Foxit PhantomPDF 被披露存在远程代码执行漏洞。攻击者可利用漏洞在当前进程的上下文中执行代码。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-2019-35803

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-2019-35413	Magento 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://magento.com/security/patches/supee-11219
CNVD-2019-35775	Dell EMC RSA Archer 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/security/zh-cn/details/DOC-106759/DSA-2019-127-RSA-Archer-Security-Update-for-Multiple-Vulnerabilities
CNVD-2019-35785	ZZZCMS zzzphp 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：http://www.zzzcms.com
CNVD-2019-35805	Apple macOS 、iCloud for Windows 和 iTunes for Windows UIFoundation 组件缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.apple.com/zh-cn/HT210634
CNVD-2019-35807	Moodle 服务器端请求伪造漏洞（CNVD-2019-35807）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://moodle.org/mod/forum/discuss.php?d=381229
CNVD-2019-35824	Electric Sheep Fencing pfsense 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.pfsense.org/security/advisories/pfSense-SA-18_08.webgui.asc
CNVD-2019-35840	多款 Bitdefender 产品代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.bitdefender.com/support/security-advisories/code-injection-bitdefender-products-windows/
CNVD-2019-35843	Linux kernel 资源管理错误漏洞（CNVD-2019-35843）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=1fb254aa983bf190cfd685d40c64a480a9bafaee
CNVD-2019-35846	Softing uaGate SI 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.softing.com
CNVD-2019-35853	Haxx curl 缓冲区溢出漏洞（CNVD-2019-35853）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://curl.haxx.se/docs/CVE-2018-1

			6839.html

小结：本周，Adobe 产品被披露存在内存错误引用漏洞，攻击者可利用漏洞执行任意代码。此外，Microsoft、WordPress、cPanel 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，执行任意代码，造成内存损坏等。另外，Foxit PhantomPDF 被披露存在远程代码执行漏洞。攻击者可利用漏洞在当前进程的上下文中执行代码。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 ACF-Frontend-Display 插件文件上传漏洞

验证描述

WordPress 是 WordPress 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。ACF-Frontend-Display 是使用在其中的一个用于在网站前端显示 ACF 表单的插件。

WordPress ACF-Frontend-Display 插件 2015-07-03 及之前版本中存在文件上传漏洞，攻击者可通过 action = upload 请求利用该漏洞将任意文件上传到 js / blueimp-jQuery-File-Upload-d45deb1 / server / php / index.php。

验证信息

POC 链接：https://packetstormsecurity.com/files/132590/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-35849

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. 小学生发现刷脸取件 bug，丰巢紧急下线人脸开锁功能

对快递公司及快递员来说，快递柜的效率大大提升了，甚至为了进一步提升取件效率，丰巢的部分快递柜上线了人脸识别功能。不过一群小学生用照片就破解了快递柜的刷脸功能，丰巢也紧急下线了刷脸取件的功能。

参考链接：https://www.cnbeta.com/articles/tech/899791.htm

2. Realtek Wi-Fi 芯片驱动漏洞能触发内核的缓冲溢出

内核的一个潜在高危漏洞允许附近恶意设备利用 Wi-Fi 信号触发崩溃或完整控制

机器。漏洞位于支持 Realtek Wi-Fi 芯片的 RTLWIFI 驱动内，当一台有 Realtek Wi-Fi 芯片的设备在恶意设备的无线电范围内，漏洞能触发内核的缓冲溢出。

参考链接：https://www.solidot.org/story?sid=62285

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