国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 6 月 18 日-2018 年 6 月 24 日 **2018 年第 25 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 217 个，其中高危漏洞 69 个、中危漏洞 143 个、低危漏洞 5 个。漏洞平均分值为 6.19。本周收录的漏洞中，涉及 0day 漏洞 75 个（占 35%），其中互联网上出现“POSCMS 'index'函数任意代码执行漏洞、Sensio Labs Symfony Web profiler 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 476 个，与上周（477 个）相比基本持平。

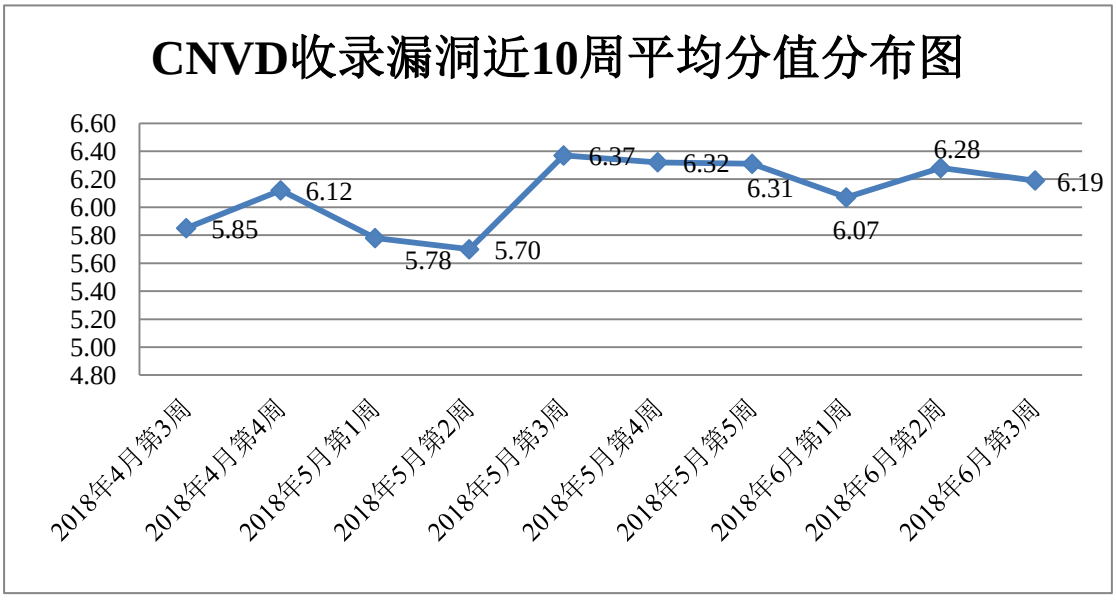

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、哈尔滨安天科技股份有限公司、新华三技术有限公司、华为技术有限公司、中国电信集团系统集成

有限责任公司等单位报送公开收集的漏洞数量较多。南京联成科技发展股份有限公司、上海谋乐网络科技有限公司、福建六壬网安股份有限公司、四川虹微技术有限公司（子午攻防实验室）、山石网科通信技术有限公司、中新网络信息安全股份有限公司、山东云天安全技术有限公司、北京明朝万达科技股份有限公司（安元实验室）、安徽锋刃信息科技有限公司、新疆海狼科技有限公司、成都思维世纪科技有限公司、河南信安世纪科技有限公司、任子行网络技术股份有限公司、上海观安信息技术股份有限公司及其他个人白帽子向 CNVD 提交了 476 个以事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和漏洞盒子向 CNVD 共享的白帽子报送的 315 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
北京天融信网络安全技术有限公司	253	0
哈尔滨安天科技股份有限公司	209	0
360 网神（补天平台）	172	172
漏洞盒子	143	143
新华三技术有限公司	124	0
华为技术有限公司	98	0
中国电信集团系统集成有限责任公司	69	0
北京神州绿盟科技有限公司	66	0
北京数字观星科技有限公司	64	0
杭州安恒信息技术有限公司	10	0
北京无声信息技术有限公司	7	0
恒安嘉新(北京)科技股份公司	6	0
厦门服云信息科技有限公司	5	0
北京知道创宇信息技术有限公司	5	2
南京联成科技发展股份有限公司	21	21

上海谋乐网络科技有限公司	7	7
福建六壬网安股份有限公司	6	6
四川虹微技术有限公司（子午攻防实验室）	5	5
山石网科通信技术有限公司	5	5
中新网络信息安全股份有限公司	5	5
山东云天安全技术有限公司	4	4
北京明朝万达科技股份有限公司（安元实验室）	2	2
安徽锋刃信息科技有限公司	2	2
新疆海狼科技有限公司	2	2
成都思维世纪科技有限公司	1	1
河南信安世纪科技有限公司	1	1
任子行网络技术股份有限公司	1	1
上海观安信息技术股份有限公司	1	1
CNCERT 吉林分中心	11	11
CNCERT 山西分中心	10	10
CNCERT 湖南分中心	6	6
CNCERT 海南分中心	2	2
CNCERT 甘肃分中心	1	1
CNCERT 广东分中心	1	1
CNCERT 宁夏分中心	1	1
CNCERT 陕西分中心	1	1
CNCERT 新疆分中心	1	1

个人	62	62
报送总计	1390	476

本周漏洞按类型和厂商统计

本周，CNVD 收录了 217 个漏洞。其中应用程序漏洞 149 个，网络设备漏洞 49 个，WEB 应用漏洞 17 个，安全产品漏洞 2 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
应用程序漏洞	149
网络设备漏洞	49
WEB 应用漏洞	17
安全产品漏洞	2

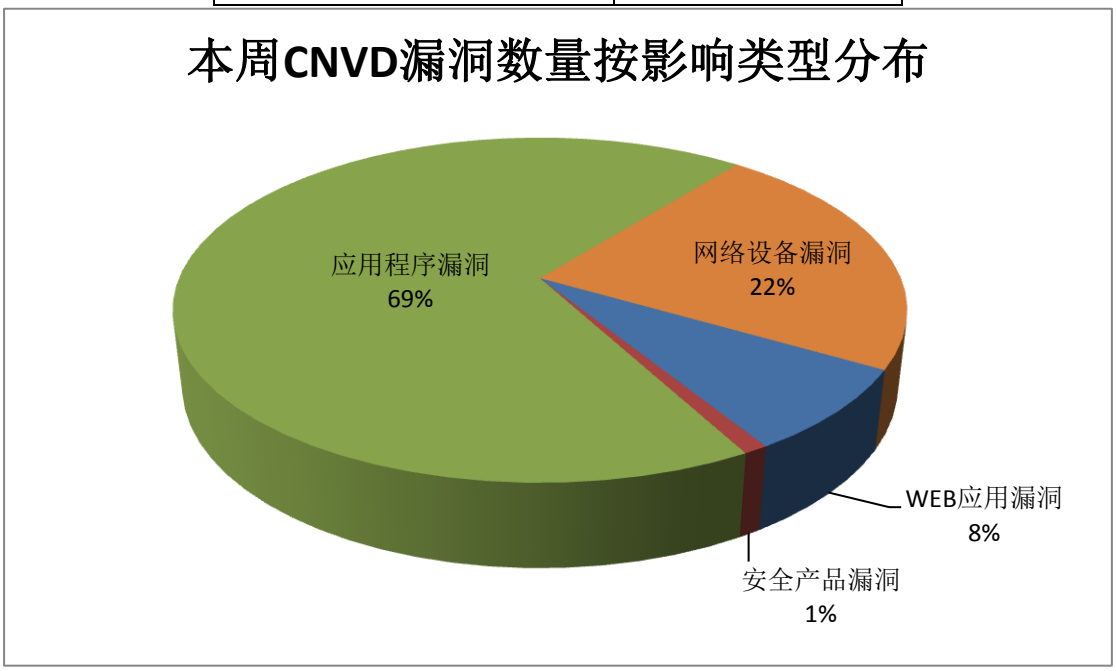

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Foxit、Microsoft 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	12%
2	Foxit	23	11%
3	MOXA	14	6%
4	Microsoft	12	6%

5	Mozilla	12	6%
6	Bouncy Castle JCE Provider	5	2%
7	Cisco	5	2%
8	Joyent	4	2%
9	CA	4	2%
10	其他	111	51%

本周行业漏洞收录情况

本周，CNVD 收录了 20 个电信行业漏洞，3 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“MULTIPROG 在处理 LST 文件存在缓冲区溢出漏洞、TP-LINK WAR302 路由器存在命令执行漏洞、Cisco FXOS 和 NX-OS Software Fabric Services 远程代码执行漏洞、Moxa EDR-810 跨站请求伪造漏洞、Moxa EDR-810 密码明文传输漏洞”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/

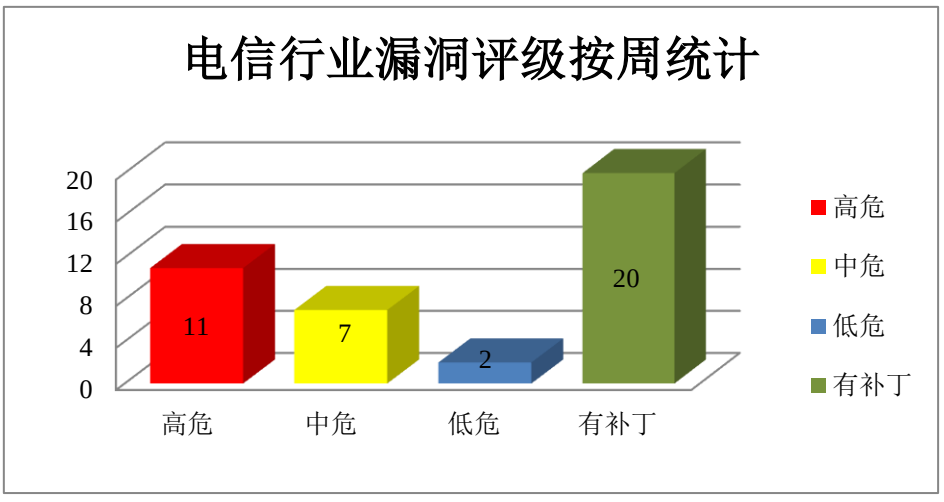

图 3 电信行业漏洞统计

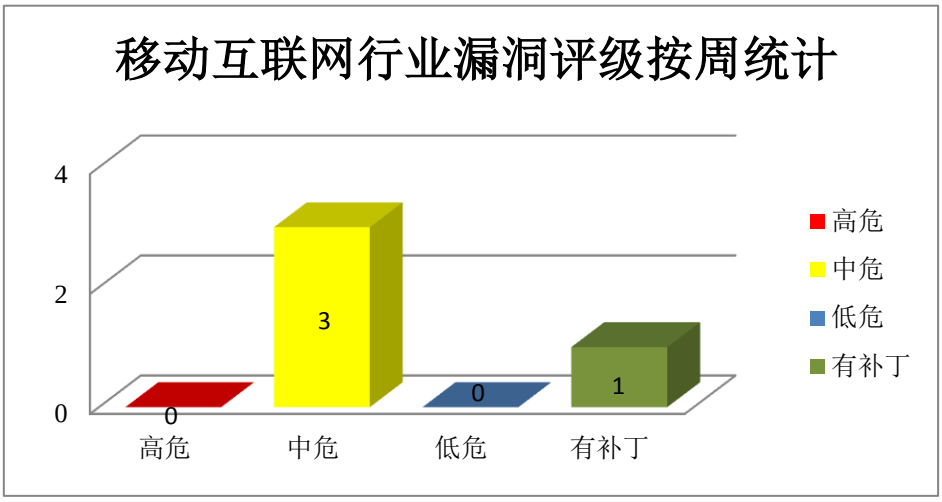

图 4 移动互联网行业漏洞统计

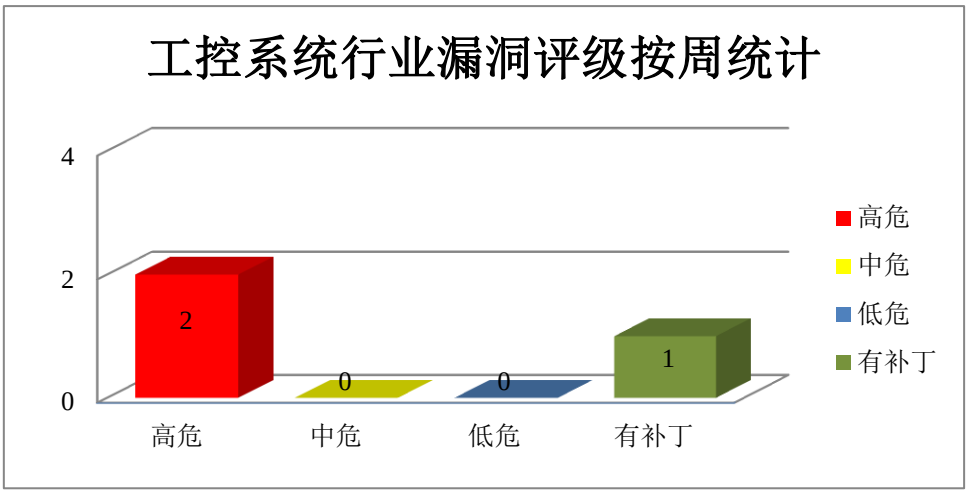

图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Acrobat 是一套 PDF 文件编辑和转换工具，Adobe Reader 一套 PDF 文档阅读软件。Adobe Flash Player 是多媒体程序播放器。Adobe Photoshop，简称“PS”，是图像处理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Photoshop 越界内存写入漏洞、Adobe Acrobat/Reader 越界写入漏洞、Adobe Acrobat/Reader 越界读取漏洞（CNVD-2018-11737）、Adobe Acrobat/Reader 内存破坏漏洞（CNVD-2018-11792）、Adobe Acrobat/Reader 类型混淆漏洞（CNVD-2018-11795）、Adobe Acrobat/Reader 不可信指针解引用漏洞、Adobe ColdFusion 不可信数据反序列化漏洞、Adobe Flash Player 类型混淆漏洞（CNVD-2018

-11803）。其中，除“Adobe Acrobat/Reader 越界读取漏洞（CNVD-2018-11737）”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-2018-11734
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11735
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11737
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11792
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11795
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11796
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11802
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11803

2、Foxit 产品安全漏洞

Foxit Reader 是一款 PDF 文档阅读器。Foxit PhantomPDF 是一个商业版。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Foxit Reader 和 PhantomPDF 远程代码执行漏洞（CNVD-2018-11901、CNVD-2018-11902、CNVD-2018-11903、CNVD-2018-11904、CNVD-2018-11905、CNVD-2018-11906、CNVD-2018-11907、CNVD-2018-11908）。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-2018-11901
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11902
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11903
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11904
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11905
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11906
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11907
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11908

3、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Firefox ESR 是 Firefox 的一个延长支持版本。Skia 是其中的一个开放源码的 2D 图形库，能够提供可在各种硬件和软件平台上工作的常见 API。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，绕过安全限制，执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Mozilla Firefox 代码执行漏洞（CNVD-2018-11787、CNVD-2018-11789）、Mozilla Firefox 安全绕过漏洞（CNVD-2018-11790）、Mozilla Firefox 信息泄露漏洞（CNVD-2018-11924、CNVD-2018-11923）、Mozilla Firefox 和 Firef

ox ESR 内存破坏漏洞（CNVD-2018-11925）、Mozilla Firefox ESR 缓冲区溢出漏洞、Mozilla Firefox ESR Skia 库内存破坏漏洞。其中，除“Mozilla Firefox 信息泄露漏洞（CNVD-2018-11924、CNVD-2018-11923）”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-2018-11787
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11789
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11790
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11924
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11923
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11925
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11927
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11928

4、Microsoft 产品安全漏洞

Microsoft Edge 是一款 Web 浏览器。Microsoft Internet Explorer 是一款网页浏览器。本周，该产品被披露存在内存破坏漏洞，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 内存破坏漏洞（CNVD-2018-11917、CNVD-2018-11918）、Microsoft Edge 和 ChakraCore 内存破坏漏洞（CNVD-2018-11919、CNVD-2018-11920）、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2018-11932、CNVD-2018-11933、CNVD-2018-11936）、Microsoft Edge 内存破坏漏洞（CNVD-2018-11935）。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-2018-11917
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11918
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11919
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11920
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11932
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11933
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11936
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11935

5、PvPGN Stats SQL 注入漏洞

PvPGN Stats 是一款基于 PHP 的支持网站与 PvPGN 游戏服务器集成的工具，它能够显示服务器状态、梯形图页面等。本周，PvPGN Stats 被披露存在 SQL 注入漏洞，远程攻击者可借助 GET 参数’user’利用该漏洞获取 PvPGN 数据库的访问权限（包括：邮

件、用户名和密码）。目前，厂商尚未发布漏洞修补程序。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-2018-11636

更多高危漏洞如表 www.cnvd.org.cn/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:// 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-2018-11715	WordPress Redirection 插件反序列化漏洞	高	用户可联系供应商获得补丁信息：https://wordpress.org/plugins/redirection/
CNVD-2018-11717	Apache Geode server 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/dc8875c0b924885a884eba6d5bd7dc3f123411b2d33cffd00e351c99@%3Cuser.geode.apache.org%3E
CNVD-2018-11836	CA Privileged Access Manager 任意命令执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.ca.com/us/product-content/recommended-reading/security-notices/ca20180614-01--security-notice-for-ca-privileged-access-manager.html
CNVD-2018-11849	Linaro LAVA 远程代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://git.linaro.org/lava/lava.git/commit/?id=583666c84ea2f12797a3eb71392bcb05782f5b14
CNVD-2018-11713	Shopify 权限提升漏洞	高	用户可联系供应商获得补丁信息：https://app.shopify.com/services/partners/dev_shops/new
CNVD-2018-11961	多款 Cisco 产品 NX-OS Software 远程代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nxos-bo
CNVD-2018-11840	VirusTotal 代码执行漏洞	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.virustotal.com/
CNVD-2018-11848	Quick Chat SQL 注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://wordpress.org/plugins/quick-chat

			/#developers
CNVD-2018-11912	redis-cli 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://github.com/antirez/redis/commit/9fdcc15962f9ff4baebe6fdd9478
CNVD-2018-11841	Carbon Black Cb Response 代码执行漏洞	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.carbonblack.com/products/cb-response/

小结：本周，Adobe 被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息，执行任意代码。此外，Foxit、Mozilla、Microsoft 等多款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，绕过安全限制，执行任意代码，造成内存破坏或发起拒绝服务攻击。另外，PvPGN Stats 被披露存在 SQL 注入漏洞，远程攻击者可借助 GET 参数’user’利用该漏洞获取 PvPGN 数据库的访问权限（包括：邮件、用户名和密码）。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。

本周漏洞要闻速递

1. 苹果的代码签名漏洞将允许恶意软件绕过多款 Mac 安全产品

近期，安全公司研究专家在 macOS 的代码签名机制中发现了一个可以利用的安全漏洞。此漏洞潜伏了一年之久，它允许攻击者将恶意的不受信任的代码伪装成受信任的合法代码，并绕过多款 macOS 安全产品的检测，其中包括 Little Snitch、F-Secure xFence、VirusTotal、Google Santa 和 Facebook OSQuery。如果你正在使用的产品出现在了上述列表中，我们建议尽快更新你所使用的产品，如果没有可用更新，请及时更换使用其他防护产品。

参考链接：http://www.freebuf.com/news/174743.html

2. FLASH 零日漏洞 CVE-2018-5002 在中东地区的定向网络攻击利用

近期，安全研究团队 (SRT) 识别出了 Adobe Flash 0 day 漏洞 CVE-2018-5002 的定向网络攻击行为，该 0 day 漏洞被攻击者用于针对中东地区重要人士和组织的网络渗透。攻击者利用该漏洞构造的恶意 Flash 对象，可以在目标受害者电脑上执行代码，实现后续渗透的一系列 Payload 和恶意代码运行。

参考链接：https://www.easyaq.com/news/2071564544.shtml

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