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 4 日-2018 年 6 月 10 日 **2018 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 212 个，其中高危漏洞 70 个、中危漏洞 127 个、低危漏洞 15 个。漏洞平均分值为 6.07。本周收录的漏洞中，涉及 0day 漏洞 59 个（占 29%），其中互联网上出现“Bitmain Antminer D3、L3+和 S9 代码执行漏洞、NUUO NVRmini 2 任意文件上传漏洞”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 630 个，与上周（465 个）环比增长 35%。

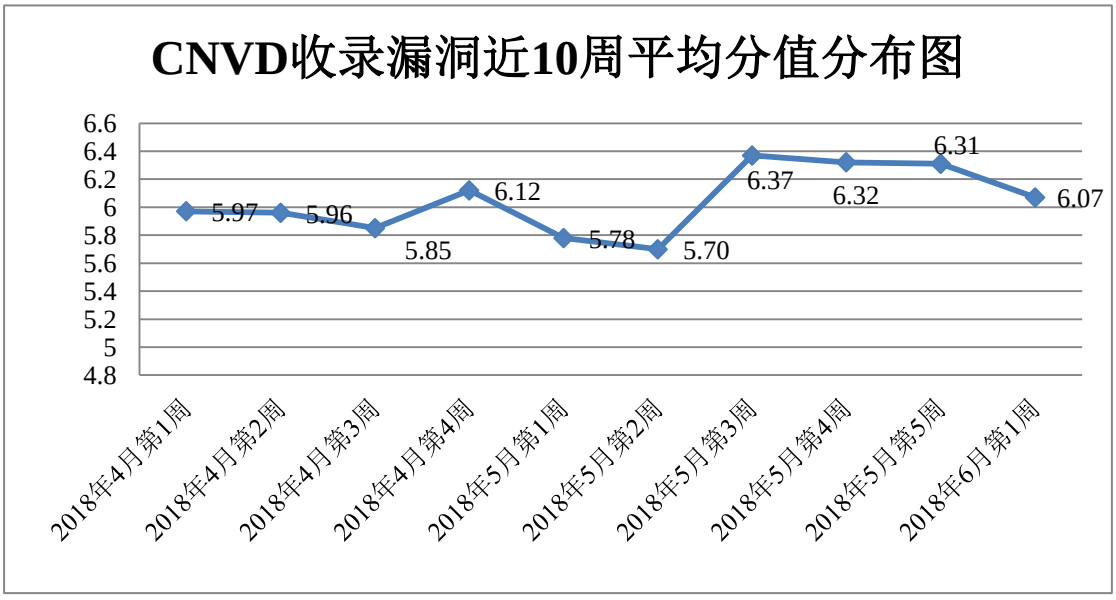

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，华为技术有限公司、哈尔滨安天科技股份有限公

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、恒安嘉新(北京)科技股份公司等单位报送公开收集的漏洞数量较多。中新网络信息安全股份有限公司、上海观安信息技术股份有限公司、四川虹微技术有限公司（子午攻防实验室）、南京联成科技发展股份有限公司、河南信安世纪科技有限公司、上海谋乐网络科技有限公司、北京同余科技有限公司、北京明朝万达科技股份有限公司（安元实验室）、中国科学院信息工程研究所、安徽锋刃信息科技有限公司、任子行网络技术股份有限公司及其他个人白帽子向 CNVD 提交了 630 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 486 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
漏洞盒子	362	362
华为技术有限公司	301	0
哈尔滨安天科技股份有限公司	262	0
北京天融信网络安全技术有限公司	140	1
新华三技术有限公司	137	0
360 网神（补天平台）	124	124
恒安嘉新(北京)科技股份公司	105	0
杭州安恒信息技术有限公司	103	0
北京神州绿盟科技有限公司	101	0
中国电信集团系统集成有限责任公司	97	0
北京数字观星科技有限公司	61	0
北京启明星辰信息安全技术有限公司	50	0
蓝盾信息安全技术有限公司	44	0
北京无声信息技术有限公司	17	0
厦门服云信息科技有限公司	10	0

北京知道创宇信息技术有限公司	1	0
中新网络信息安全股份有限公司	9	9
上海观安信息技术股份有限公司	8	8
四川虹微技术有限公司（子午攻防实验室）	5	5
南京联成科技发展股份有限公司	3	3
河南信安世纪科技有限公司	3	3
上海谋乐网络科技有限公司	2	2
北京同余科技有限公司	2	2
北京明朝万达科技股份有限公司（安元实验室）	2	2
中国科学院信息工程研究所	2	2
安徽锋刃信息科技有限公司	1	1
任子行网络技术股份有限公司	1	1
CNCERT 吉林分中心	2	2
CNCERT 贵州分中心	2	2
CNCERT 甘肃分中心	1	1
CNCERT 河北分中心	1	1
CNCERT 内蒙古分中心	1	1
CNCERT 宁夏分中心	1	1
个人	97	97
报送总计	2058	630

本周漏洞按类型和厂商统计

本周，CNVD 收录了 212 个漏洞。其中应用程序漏洞 142 个，WEB 应用漏洞 24 个，网络设备漏洞 22 个，操作系统漏洞 16 个，安全产品漏洞 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
应用程序漏洞	142
WEB 应用漏洞	24
网络设备漏洞	22
操作系统漏洞	16
安全产品漏洞	8

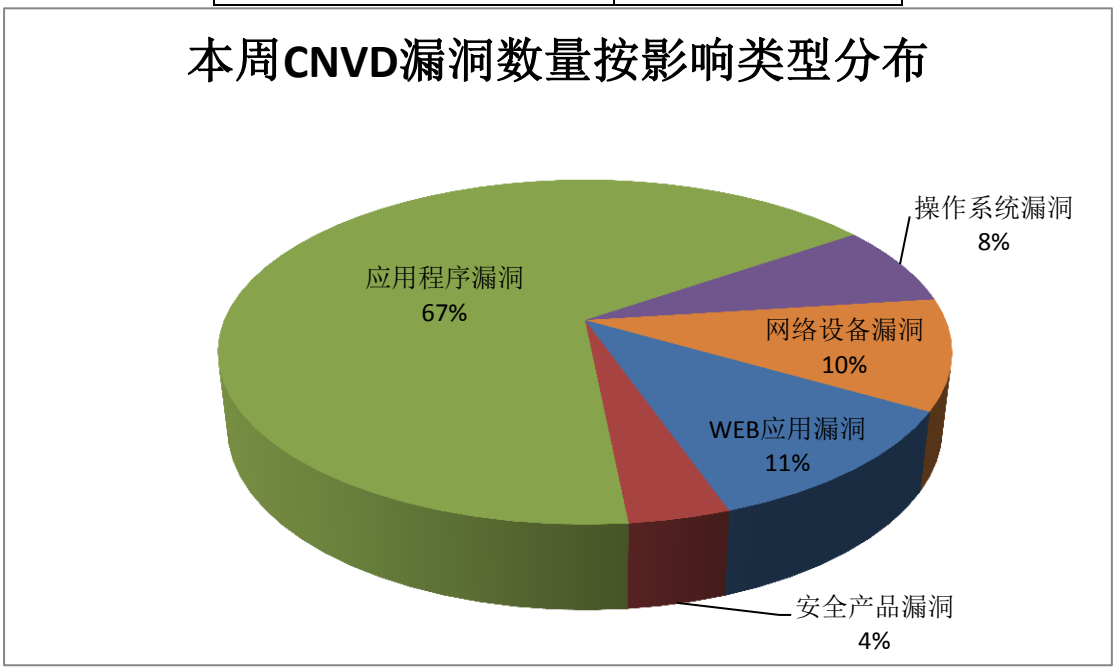

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Oracle、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	Microsoft	18	9%
2	Oracle	15	7%
3	Adobe	11	5%
4	IBM	10	5%
5	Espruino	9	4%
6	Libmobi	7	3%
7	CloudBees	5	2%
8	Foxit	4	2%
9	Schneider Electric	4	2%
10	其他	129	61%

本周行业漏洞收录情况

本周，CNVD 收录了 7 个电信行业漏洞，6 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“GE MDS PulseNET and MDS PulseNET Enterprise 远程代码执行漏洞、JCG-AC836 捷稀路由器安卓客户端存在拒绝服务漏洞、JCG-AC836M 捷稀路由器安卓客户端存在信息泄露漏洞”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/

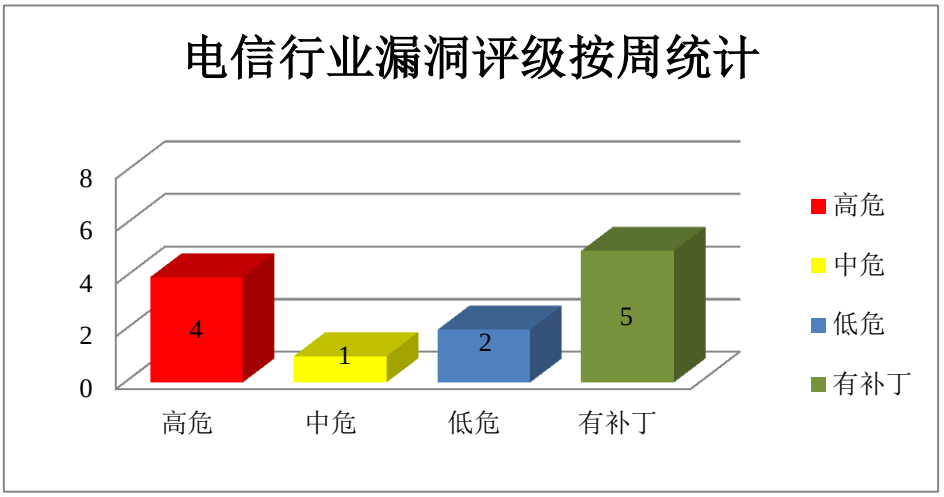

图 3 电信行业漏洞统计

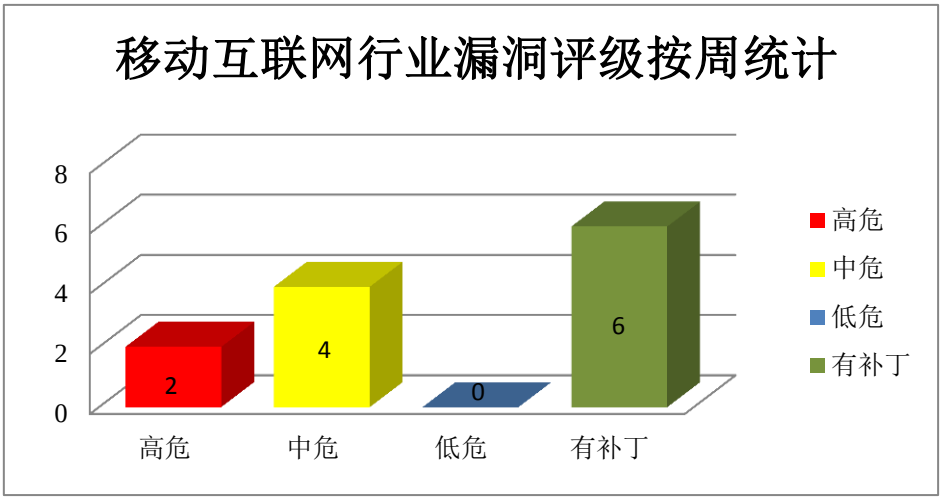

图 4 移动互联网行业漏洞统计

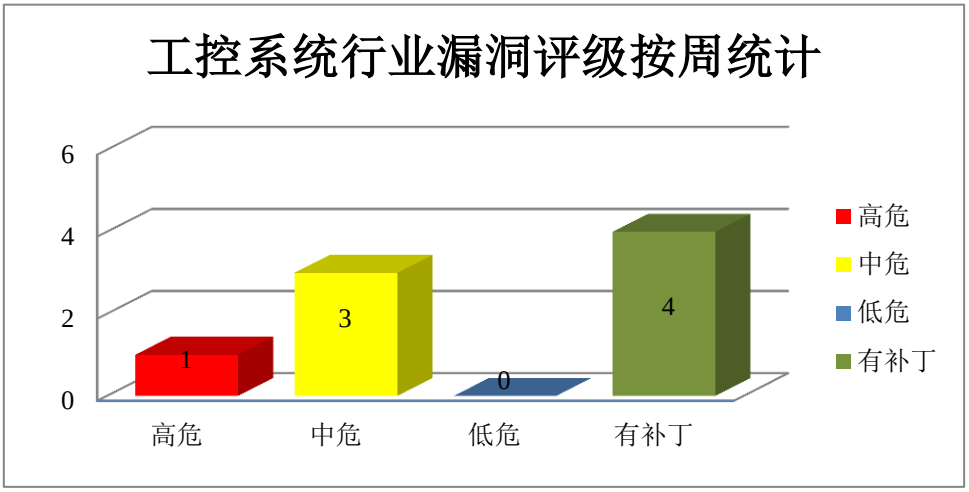

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Office 2016 for Mac 是美国微软（Microsoft）公司开发的一款基于 Mac 平台的办公软件套件产品。PowerPoint 是 Office 套件中的一个文档演示工具。Microsoft Windows 是美国微软公司研发的一套操作系统，Windows 采用了图形化模式 GUI。Microsoft SharePoint Enterprise Server 2013 SP1、SharePoint Enterprise Server 2016 和 SharePoint Server 2010 SP2 都是企业业务协作平台，用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。Access 是其中的一个数据库组件。本周，上述产品被披露存在权限提升和远程代码执行漏洞，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 PowerPoint 远程代码执行漏洞（CNVD-2018-10942）、Microsoft Windows 权限提升漏洞（CNVD-2018-10982）、Microsoft Windows Win32k 权限提升漏洞（CNVD-2018-10986、CNVD-2018-10987）、Microsoft Windows 远程代码执行漏洞（CNVD-2018-10992、CNVD-2018-11048）、Microsoft SharePoint Server 权限提升漏洞（CNVD-2018-11000）、Microsoft Windows Image 权限提升漏洞，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-2018-10942

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10982

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10986

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10987

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10992

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11048

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11000

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11047

2、Adobe 产品安全漏洞

Adobe Acrobat 和 Reader 都是美国奥多比（Adobe）公司的产品。前者是一套 PDF 文件编辑和转换工具，后者是一套 PDF 文档阅读软件。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任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 堆溢出漏洞（CNVD-2018-10976、CNVD-2018-10977、CNVD-2018-10978）、Adobe Acrobat/Reader 缓冲区溢出漏洞（CNVD-2018-10886、CNVD-2018-10996、CNVD-2018-10998、CNVD-2018-10997、CNVD-2018-10999）。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-2018-10976

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10977

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10978

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10886

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10996

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10998

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10997

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10999

3、IBM 产品安全漏洞

IBM API Connect（又名 APIConnect）是美国 IBM 公司的一套用于管理 API 生命周期的集成解决方案。IBM BigFix Platform 是一款系统管理软件。IBM InfoSphere Information Server 是市场领先的数据集成平台，其中包括一系列产品。IBM SAN Volume Controller（SVC）是存储系统。IBM SVC 是一套虚拟化存储系统；Storwize 是一套专为中小型企业定制的磁盘存储系统；Spectrum Virtualize 是一套光谱存储系统；FlashSystem 是一套全闪存存储系统。本周，上述产品被披露存在信息泄露和权限提升漏洞，攻击者可利用漏洞获取敏感信息或提升权限。

CNVD 收录的相关漏洞包括：IBM API Connect 信息泄露漏洞（CNVD-2018-10950）、IBM InfoSphere Information Server 权限提升漏洞、IBM BigFix Platform 信息泄露漏洞（CNVD-2018-11073）、IBM InfoSphere Information Server 信息泄露漏洞（CNVD-2018-11080）、多款 IBM 产品信息泄露漏洞（CNVD-2018-11111、CNVD-2018-11110、CNVD-2018-11113、CNVD-2018-11112）。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-2018-10950

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11072

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11073

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11080

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11111

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11110

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11113

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11112

4、Oracle 产品安全漏洞

Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的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。Oracle Hospitality Applications 是一套用于酒店管理的业务应用程序、服务器和存储解决方案。Oracle Retail Applications 是一套零售应用商店解决方案。本周，该产品被披露存在拒绝服务和未授权操作漏洞，攻击者可利用漏洞未授权访问、更新、插入或删除数据或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Oracle Fusion Middleware Outside In Technology 组件拒绝服务漏洞（CNVD-2018-10966、CNVD-2018-10969）、Oracle Fusion Middleware WebCenter Content 组件未授权操作漏洞、Oracle Fusion Middleware Data Visualization Desktop 组件拒绝服务漏洞、Oracle Hospitality Applications Hospitality Suite8 组件拒绝服务漏洞、Oracle Retail Applications Retail Integration Bus 组件未授权操作漏洞、Oracle Retail Applications Retail Back Office 组件未授权操作漏洞、Oracle Retail Applications Retail Point-of-Service 组件未授权操作漏洞。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-2018-10966

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10969

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10993

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10994

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10995

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11039

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11042

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11041

5、D-Link DIR-816 A2 栈缓冲区溢出漏洞

D-Link DIR-816 A2 是友讯（D-Link）公司的一款无线路由器产品。GoAhead 是其中的一款嵌入式 Web 服务器。本周，D-Link 被披露存在栈缓冲区溢出漏洞，远程攻击者可通过发送带有较长 HTTP Host 包头的请求利用该漏洞执行任意代码。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-2018-10930

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-2018-11129	Schneider Electric MGE UPS 和 MGE STS 66074 MGE Network Management Card Transverse 信息泄露漏洞	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.schneider-electric.com/en/download/document/SEVD-2018-074-01/
CNVD-2018-11076	多款 Huawei 服务器身份验证绕过漏洞	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.huawei.com/cn/psirt/security-advisories/huawei-sa-20180530-01-server-cn
CNVD-2018-11077	多款 TP-LINK 产品访问控制错误漏洞	高	无
CNVD-2018-11035	OpenDaylight Controller SQL 注入漏洞	高	无
CNVD-2018-10968	ASUSTOR ADM 存在多个漏洞	高	用户可联系供应商获得补丁信息：https://www.purehacking.com/blog/matthew-fulton/back-to-the-future-asustor-web-exploitation
CNVD-2018-11023	Synology Drive 访问控制错误漏洞	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.synology.cn/en-global/support/security/Synology_SA_18_11
CNVD-2018-10896	dalek-browser-chrome-canary 代码执行漏洞	高	无
CNVD-2018-10908	Quest KACE System Management Appliance 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：https://support.quest.com/download-install-detail/6086148
CNVD-2018-10972	Activision Blizzard Infinity Ward Call of Duty Modern Warfare 2 缓冲区溢出漏洞	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.activision.com/company/locations/infinity-ward
CNVD-2018-11075	VMware Horizon Client for Linux 权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://my.vmware.com/en/web/vmware/info/slug/desktop_end_user_computing

			/vmware_horizon_clients/4_0

小结：本周，Microsoft 被披露存在权限提升和远程代码执行漏洞，攻击者可利用漏洞提升权限、执行任意代码。此外，Adobe、IBM、Oracle 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、提升权限、执行任意代码或发起拒绝服务攻击等。另外，D-Link 被披露存在栈缓冲区溢出漏洞，远程攻击者可通过发送带有较长 HTTP Host 包头的请求利用该漏洞执行任意代码。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。

本周漏洞要闻速递

1. Windows 系统的 JScript 组件被曝存在一个 0day RCE

近期，Telspace Systems 公司的安全研究专家 Dmitri Kaslov 在 Windows 操作系统的 JScript 组件中发现了一个严重的安全漏洞，而这个漏洞将允许攻击者在目标主机上执行恶意代码。目前，该漏洞的 CVSSv2 严重等级评估为 6.8 分（10）。在利用该漏洞实施攻击的过程中，攻击者需要欺骗用户访问特定的恶意 Web 页面，或在主机中下载并打开恶意 JS 文件。

参考链接：http://www.freebuf.com/articles/system/174187.html

2. Zip Slip 漏洞影响大量项目，范围横跨多个生态系统

近日，研究人员披露了一个关键漏洞，能够影响众多涉及压缩文件的开源库。在软件解压压缩包时会受此漏洞影响，压缩文件的种类包括：tar、jar、war、cpio、apk、rar 和 7z。Zip Slip 漏洞是“任意文件覆盖”以及“目录遍历”的结合，攻击者可以把文件解压到敏感位置，从而覆盖掉系统文件或者服务器配置。各种编程语言的压缩库都收到影响，其中 Java 生态系统影响最为严重。不过这个漏洞更偏重理论而非一个真正的漏洞。

参考链接：https://www.bleepingcomputer.com/news/security/zip-slip-vulnerability-affects-thousands-of-projects-across-multiple-ecosystems/

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