国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 01 月 21 日-2019 年 01 月 27 日　　2019 年第 4 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 177 个，其中高危漏洞 65 个、中危漏洞 94 个、低危漏洞 18 个。漏洞平均分值为 6.01。本周收录的漏洞中，涉及 0day 漏洞 46 个（占 26%），其中互联网上出现“D-Link DIR-818LW Rev.A 和 DIR-860L Rev.B 操作系统命令注入漏洞、Webmin 远程命令执行漏洞”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 1638 个，与上周（1501 个）环比增长 9%。

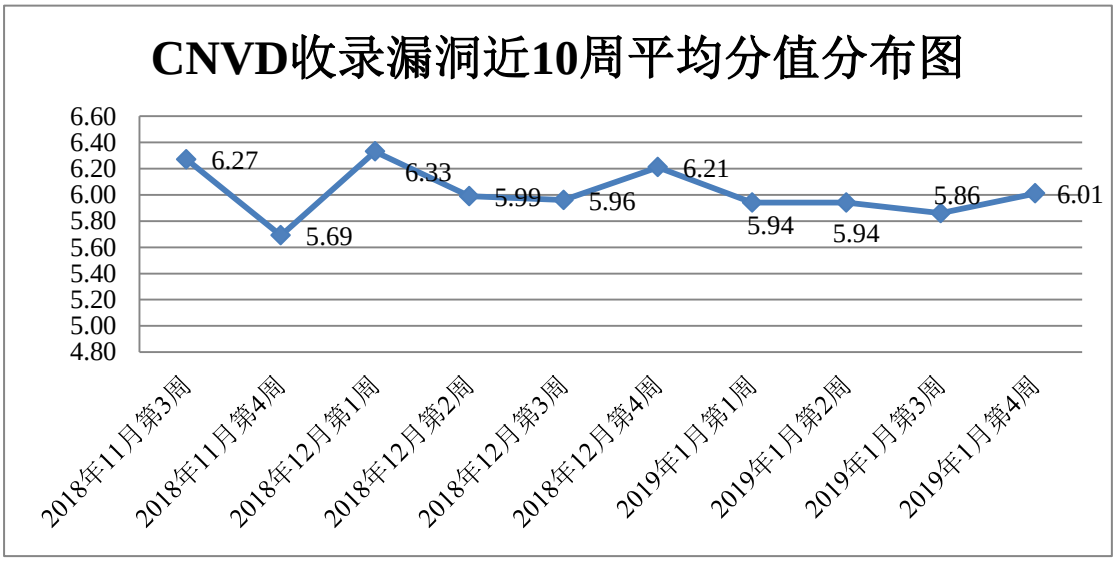

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 8 起，向银行、保险、能源等重要行业单位通报漏洞事件 44 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 353 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 549 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15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：

飞利浦（中国）投资有限公司、西安摩高互动科技有限公司、厦门正航软件科技有限公司、青岛商至信网络科技有限公司、宝简好网络科技有限公司、浙江宇视科技有限公司、厦门服云信息科技有限公司、淄博闪灵网络科技有限公司、淮南市银泰软件科技有限公司、上海商创网络科技有限公司、长城宽带网络服务有限公司北京分公司、中国知网、企炬中国、御宅男工作室、亿渡留言管理系统、梦想 CMS、LaySNS、CLTPHP、zzcms、EasyCMS 和 Joomla。

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、新华三技术有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。天津市国瑞数码安全系统股份有限公司、山东云天安全技术有限公司、安徽锋刃信息科技有限公司、中新网络信息安全股份有限公司、任子行网络技术股份有限公司、北京国舜科技股份有限公司、河南信安世纪科技有限公司、北京山石网科信息技术有限公司、广州竞远安全技术股份有限公司、南京联成科技发展股份有限公司、普华永道商务咨询(上海)有限公司广州分公司、上海零盾网络科技有限公司及其他个人白帽子向 CNVD 提交了 1638 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1043 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）	599	599
360 网神（补天平台）	444	444
北京天融信网络安全技术有限公司	226	14
哈尔滨安天科技集团股份有限公司	161	0
华为技术有限公司	153	0
新华三技术有限公司	72	0
北京神州绿盟科技有限公司	69	0

中国电信集团系统集成有限责任公司	69	2
北京数字观星科技有限公司	66	0
北京启明星辰信息安全技术有限公司	49	0
恒安嘉新(北京)科技股份公司	19	0
深信服科技股份有限公司	4	4
北京知道创宇信息技术有限公司	3	0
天津市国瑞数码安全系统股份有限公司	248	248
山东云天安全技术有限公司	50	50
安徽锋刃信息科技有限公司	48	48
中新网络信息安全股份有限公司	43	43
任子行网络技术股份有限公司	19	19
北京国舜科技股份有限公司	9	9
河南信安世纪科技有限公司	9	9
北京山石网科信息技术有限公司	4	4
广州竞远安全技术股份有限公司	3	3
南京联成科技发展股份有限公司	3	3
普华永道商务咨询(上海)有限公司广州分公司	1	1
上海零盾网络科技有限公司	1	1
CNCERT 湖南分中心	4	4
CNCERT 贵州分中心	3	3
CNCERT 河北分中心	2	2
CNCERT 吉林分中心	2	2

个人	126	126
报送总计	2509	1638

本周漏洞按类型和厂商统计

本周，CNVD 收录了 177 个漏洞。应用程序漏洞 121 个，网络设备漏洞 20 个，操作系统漏洞 17 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	121
网络设备漏洞	20
操作系统漏洞	17
WEB 应用漏洞	17
安全产品漏洞	2

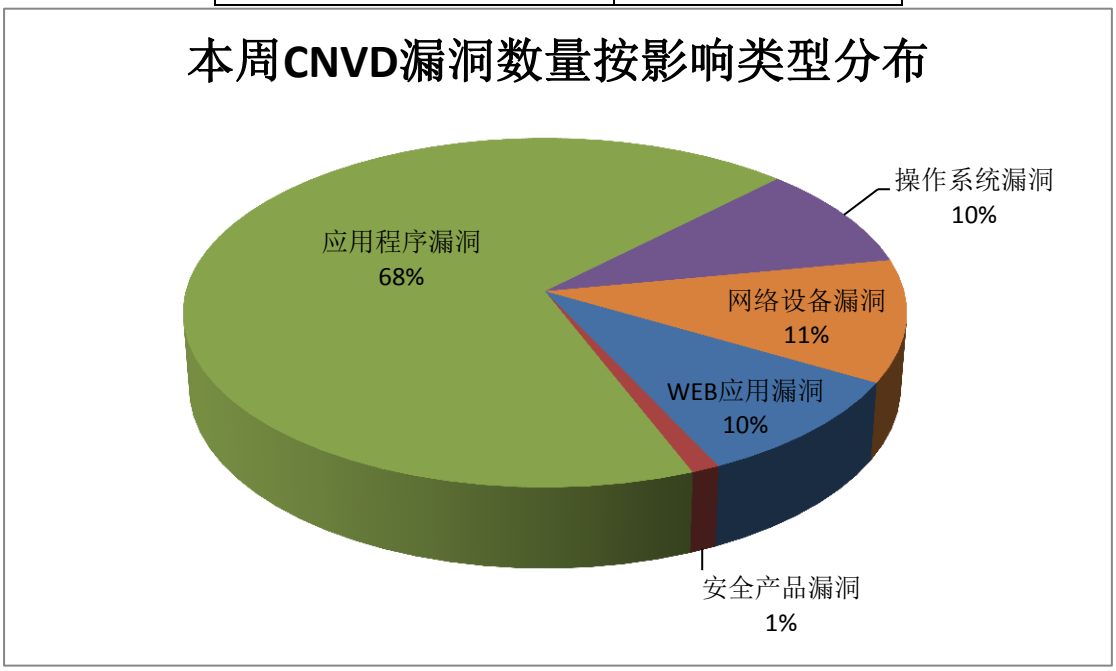

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Cisco、FFmpeg 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	Cisco	16	9%
3	FFmpeg	11	6%

4	Red Hat	11	6%
5	xkbcommon	11	6%
6	Apache	9	5%
7	Apple	8	5%
8	Intel	7	4%
9	D-Link	6	3%
10	其他	76	43%

本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，10 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“LCDS LAquis SCADA 代码注入漏洞、多款 Apple 产品越界读取漏洞（CNVD-2019-02759）、Cisco Small Business RV320 和 RV325 信息泄露漏洞、LAquis SCADA 输入验证漏洞、多款 Apple 产品沙盒绕过漏洞、Cisco Small Business RV320 和 RV325 命令注入漏洞”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/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

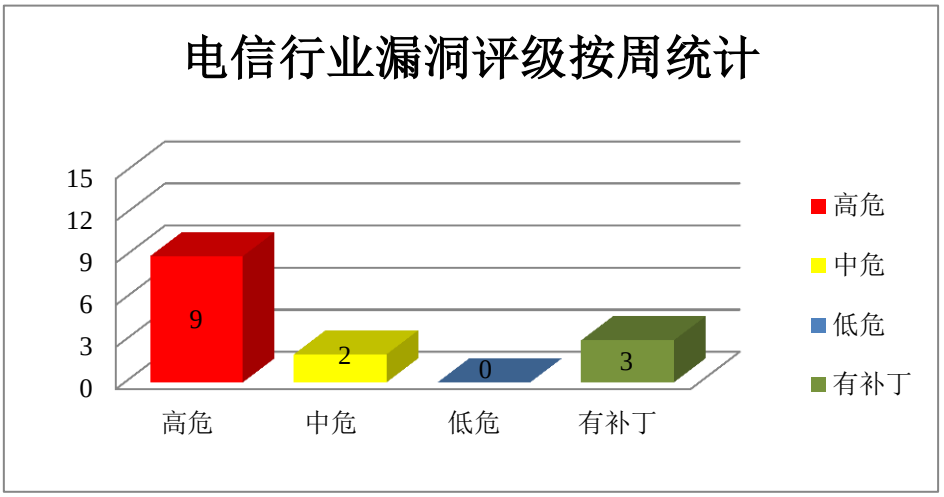

图 3 电信行业漏洞统计

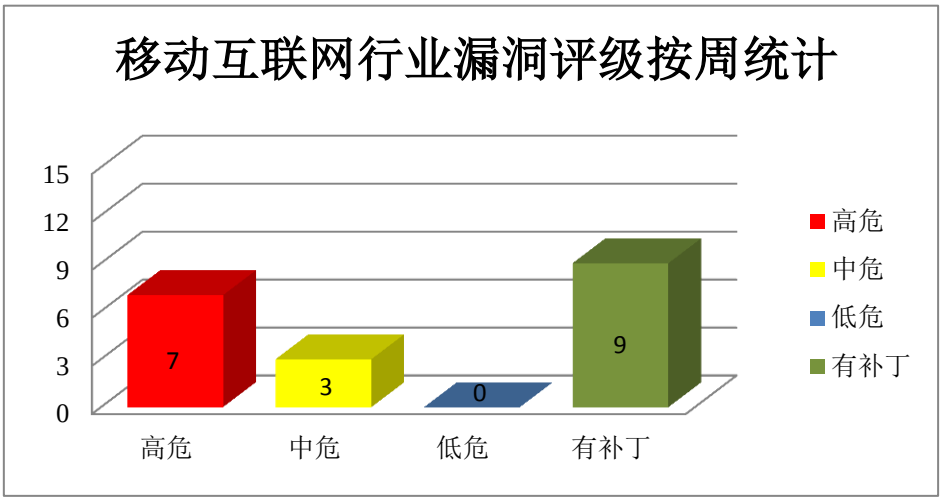

图 4 移动互联网行业漏洞统计

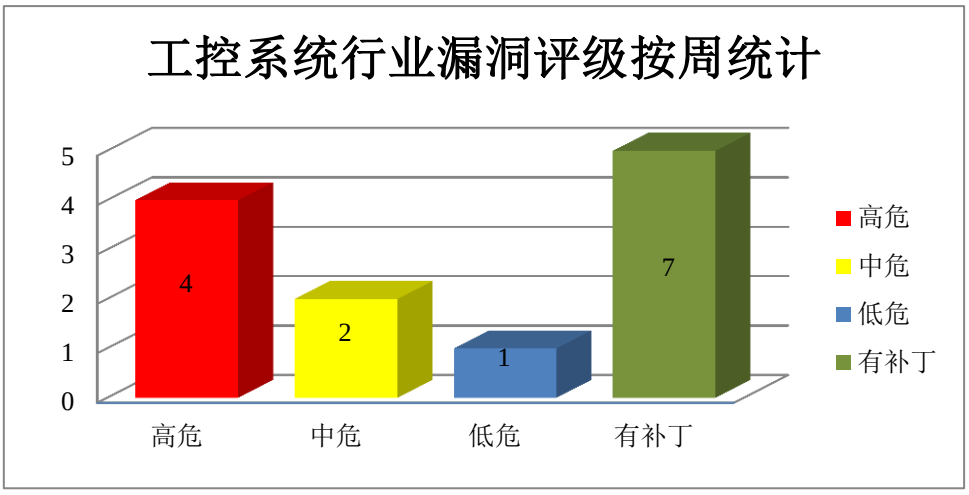

图 5 工控系统行业漏洞统计

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 Windows 7 SP1 是一套个人电脑使用的操作系统。Microsoft Windows 10 是一套供个人电脑使用的操作系统.Windows Server 2016 是一套服务器操作系统。Windows Server 2008 SP2 是一套服务器操作系统。Microsoft Windows Server 2012 R2 等都是美国微软（Microsoft）公司发布的一系列服务器操作系统。Microsoft Project 是一套适用于项目组合管理（PPM）和日常工作的项目管理解决方案。该方案支持为任务分配资源、进度跟踪和预算管理等。Microsoft Internet Explorer（IE）是一款 Web 浏览器。Office 2010 SP2 是一套办公套件。Microsoft MSHTML engine 是其中的一个用于解析 HTML 语言的引擎。Microsoft Excel 是微软公司的办公软件 Microsoft office 的组件之一，是由 Microsoft 为 Windows 和 Apple Macintosh 操作系统的电脑而编写和运行的一款试算

表软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD收录的相关漏洞包括：Microsoft DirectX权限提升漏洞（CNVD-2019-02495）、Microsoft Windows 跨站脚本漏洞（CNVD-2019-02770）、Microsoft Graphics 远程代码执行漏洞、Microsoft Windows 权限提升漏洞（CNVD-2019-02775）、Microsoft Project 远程代码执行漏洞、Microsoft MSHTML 引擎输入验证漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2019-02780、CNVD-2019-02784）。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-2019-02495

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02770

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02768

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02775

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02776

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02777

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02780

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02784

2、Cisco 产品安全漏洞

Cisco Small Business RV320 和 RV325 都是美国思科（Cisco）公司的企业级路由器。Cisco SD-WAN Solution 是运行在思科系统上的一套网络扩展解决方案。Cisco Webex Business Suite WBS32 sites 等都是美国思科（Cisco）公司的视频会议解决方案。Cisco Webex Network Recording Player 和 Webex Player 都是其中的用于播放视频会议记录的播放器。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：Cisco Small Business RV320和RV325命令注入漏洞、Cisco Small Business RV320和RV325信息泄露漏洞、Cisco SD-WAN Solution缓冲区溢出漏洞、Cisco Webex Network Recording Player和Webex Player for Windows缓冲区溢出漏洞（CNVD-2019-02786、CNVD-2019-02787、CNVD-2019-02788、CNVD-2019-02789、CNVD-2019-02790）。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-2019-02747

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02748

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02754

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02786

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02787

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02788

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02789

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02790

3、Apple 产品安全漏洞

Apple iOS 是为移动设备所开发的一套操作系统；Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器；tvOS 是一套智能电视操作系统；watchOS 是一套智能手表操作系统；iCloud for Windows 是一款基于 Windows 平台的云服务。macOS Mojave 是一套为 Mac 计算机所开发的专用操作系统。Apple macOS High Sierra 是美国苹果（Apple）公司的一套专为 Mac 计算机所开发的专用操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过沙盒限制，注入任意的 Web 脚本或 HTML，提升权限，执行任意代码（内存破坏）。

CNVD 收录的相关漏洞包括：多款 Apple 产品内存破坏漏洞（CNVD-2019-02753）、多款 Apple 产品沙盒绕过漏洞、多款 Apple 产品跨站脚本漏洞（CNVD-2019-02756）、多款 Apple 产品沙盒绕过漏洞（CNVD-2019-02757）、多款 Apple 产品越界读取漏洞（CNVD-2019-02758、CNVD-2019-02759、CNVD-2019-02760、CNVD-2019-02761）。其中，除“多款 Apple 产品跨站脚本漏洞（CNVD-2019-02756）”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-2019-02753

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02755

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02756

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02757

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02758

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02759

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02760

http://www.cnvd.org.cn/flaw/show/CNVD-2019-02761

4、Red Hat 品安全漏洞

Red Hat 389 Directory Server（前称 Fedora Directory Server）是一款企业级的 Linux 目录服务器。Red Hat Gluster 是一套开源的分布式文件系统。Red Hat Gluster Storage 是一个用于软件的横向扩展存储软件包，它能够提供非结构化的数据存储方式。Red Hat Ceph Storage 是一套可扩展的、开放性的软件定义存储平台。Red Hat PolicyKit（又名 Polkit）是一个用于在 Unix 兼容系统中对应用程序进行权限控制的工具。Red Hat Ceph 是一套 Linux PB 级分布式文件系统。Red Hat Virtualization 是推出的一套针对服务器和桌面的虚拟化管理解决方案（企业虚拟化平台），它可提供实时迁移、负载平衡等功能。Red Hat Virtualization Host 是一款虚拟主机。本周，该产品被披露存在多个

漏洞，攻击者可利用漏洞绕过保护机制，执行未授权操作，执行任意命令，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Red Hat 389 Directory Server 拒绝服务漏洞（CNVD-2019-02473）、Red Hat Gluster 未授权操作漏洞、Red Hat Gluster Storage glusterfs server 拒绝服务漏洞、Red Hat Ceph Storage ceph-isci-cli 包远程命令注入漏洞、Red Hat PolicyKit 未授权访问漏洞、Red Hat Ceph 未授权访问漏洞、Red Hat Ceph 拒绝服务漏洞（CNVD-2019-02480）、Red Hat Virtualization 和 Virtualization Host 拒绝服务漏洞。其中，“Red Hat 389 Directory Server 拒绝服务漏洞（CNVD-2019-02473）、Red Hat Gluster 未授权操作漏洞、Red Hat Ceph Storage ceph-isci-cli 包远程命令注入漏洞”的综合评级为“高危”。目前，除“Red Hat 389 Directory Server 拒绝服务漏洞（CNVD-2019-02473）”外，厂商已经发布了其余漏洞的修补程序。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-2019-02473
http://www.cnvd.org.cn/flaw/show/CNVD-2019-02475
http://www.cnvd.org.cn/flaw/show/CNVD-2019-02476
http://www.cnvd.org.cn/flaw/show/CNVD-2019-02477
http://www.cnvd.org.cn/flaw/show/CNVD-2019-02478
http://www.cnvd.org.cn/flaw/show/CNVD-2019-02479
http://www.cnvd.org.cn/flaw/show/CNVD-2019-02480
http://www.cnvd.org.cn/flaw/show/CNVD-2019-02507

5、Apache HTTP Server 拒绝服务漏洞

Apache HTTP Server 是美国阿帕奇（Apache）软件基金会的一款开源网页服务器。本周，Apache HTTP Server 被披露存在拒绝服务。攻击者可利用该漏洞造成拒绝服务。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-2019-02938

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-2019-02383	Huawei PCManager 权限提升漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20190109-01-pcmanager-cn
CNVD-2019-02384	LAquis SCADA 输入验证漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://laquisscada.com/
CNVD-2019-02492	Google gVisor 文件重命名漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://github.com/google/gvisor/commit/001a4c2493b13a43d62c7511fb509a959ae4abc2#diff-94321190b0a3f6b9808390d4102b65e90
CNVD-2019-02500	多款 Fuji Xerox 产品命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://securitydocs.business.xerox.com/wp-content/uploads/2018/12/cert_Security_Mini_Bulletin_XRX18AL_for_ALB80xx-C80xx_v1.1.pdf
CNVD-2019-02506	HPE Intelligent Management Center 缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03906en_us
CNVD-2019-02509	Intel PROSet/Wireless WiFi Software 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://downloadcenter.intel.com/product/72252/Intel-PROSet-Wireless-Software
CNVD-2019-02521	Devellion CubeCart 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://www.cubecart.com/
CNVD-2019-02524	WordPress Automattic WooCommerce 插件文件删除漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://automattic.com/wordpress-plugins/
CNVD-2019-02530	PgpoolAdmin 未授权访问漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://pgpool.net/mediawiki/index.php/Main_Page
CNVD-2019-02752	Linux apt/apt-get 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://security-tracker.debian.org/tracker/CVE-2019-3462

小结：本周，Microsoft 被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。此外，Cisco、Apple、Red Hat 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，绕过沙盒限制，执行未授权操作，注入任意的 Web 脚本或 HTML，提升权限，执行任意代码（内存破坏），发起拒绝服务攻击等。另外，Apache HTTP Server 被

披露存在拒绝服务漏洞。攻击者可利用该漏洞造成拒绝服务。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、D-Link DIR-818LW Rev.A 和 DIR-860L Rev.B 操作系统命令注入漏洞

验证描述

D-Link DIR-818LW Rev.A 和 DIR-860L Rev.B 都是友讯（D-Link）公司的无线路由器产品。

D-Link DIR-818LW Rev.A 2.05.B03 版本和 DIR-860L Rev.B 2.03.B03 版本中的 cgibin 二进制文件的 soap.cgi 服务存在命令注入漏洞。远程攻击者可借助‘service’参数中的“&&”子字符串利用该漏洞执行 shell 命令。

验证信息

POC 链接：https://github.com/pr0v3rbs/CVE/tree/master/CVE-2018-20114

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-02503

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. Linux APT 包管理器中的严重缺陷可能导致远程黑客入侵

Linux APT 包管理器是个广泛使用的程序，用于处理 Debian、Ubuntu 和其他 Linux 发行版上软件的安装、更新和删除等行为。近日，有安全专家披露 Linux APT 包管理器中存在严重远程代码执行漏洞。由于存在漏洞的版本在 HTTP 重定向期间没有正确清理某些参数，远程中间人攻击者可以注入恶意内容并诱导系统安装被恶意更改的软件包。目前，Linux APT 包管理器更新版本（1.4.9）已经发布，相关用户可尽快更新。

参考链接：https://thehackernews.com/2019/01/linux-apt-http-hacking.html

2. Exchange 提权漏洞预警（CVE-2018-8581）

近日，国外安全研究员 dirkjanm 通过博客文章公布了 Exchange 服务器上的一个提权漏洞的利用详情，漏洞编号为 CVE-2018-8581，实际上该漏洞早于去年 12 月份由 ZERO DAY INITIATIVE 组织发布的一篇技术博客中批露。该漏洞利用了 Exchange 服务器的 SSRF 和高权限的请求，导致拥有合法邮箱凭证的用户可以被提升至域管权

限。目前，微软对该漏洞并未发布任何补丁，只提供了缓解该攻击的手法，但该方法也并不适用于所有的 Exchange 服务器。

参考链接：https://www.freebuf.com/vuls/194857.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