国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 9 月 10 日-2018 年 9 月 16 日 **2018 年第 37 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 301 个，其中高危漏洞 117 个、中危漏洞 161 个、低危漏洞 23 个。漏洞平均分值为 6.07。本周收录的漏洞中，涉及 0day 漏洞 66 个（占 22%），其中互联网上出现“Netgate Registry Clenaner 本地权限提升漏洞、Manage Engine Exchange Reporter Plus 远程代码执行漏洞”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 1267 个，与上周（711 个）环比增长 78%。

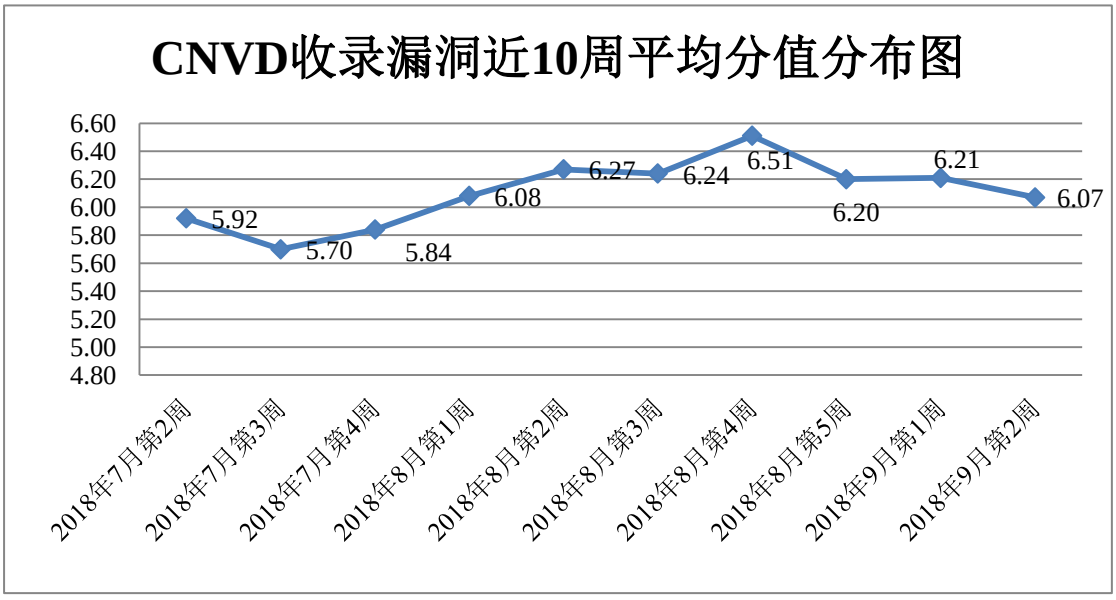

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 18 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 199 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 123 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 16 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：

中电环保股份有限公司、天辉网络服务有限公司、合肥市一新软件开发有限责任公司、富士施乐(中国)有限公司、语联网（武汉）信息技术有限公司、上海璞鼎文化传播有限公司、青岛软媒网络科技有限公司、哈尔滨伟成科技有限公司、北京江民新科技术有限公司、河南亿普格计算机科技有限公司、四川方法数码科技有限公司、广东省交通集团有限公司、淄博闪灵网络科技有限公司、微点佰慧(北京)信息安全技术有限公司、中国软件与技术服务股份有限公司、杭州翰臣科技有限公司、成都康菲顿特网络科技有限公司、上海德米萨信息科技有限公司、北京辰信领创信息技术有限公司、太原迅易科技有限公司、南昌蓝智科技有限公司、广州世安信息技术有限公司、漳州豆壳网络科技有限公司、北京经纬中天信息技术有限公司、施耐德（Schneider Electric）、北京市计算中心、凤凰网财经、中国橡胶工业协会乳胶分会、中华民国劳资关系服务协会、深圳市机械行业协会、中国国画院、中国医学科学院医学生物学研究所、北京供暖宣传网、中国旅游投资网、中国专利展示网、EHS 环境安全法规网、中国创业人才测评网、中国发明专利技术信息网、SaxueCMS、zzzcms。

本周，CNVD 发布了《Microsoft 发布 2018 年 9 月安全更新》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4679

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技股份有限公司、蓝盾信息安全技术有限公司、新华三技术有限公司、北京天融信网络安全技术有限公司、华为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、北京圣博润高新技术股份有限公司、南京联成科技发展股份有限公司、任子行网络技术股份有限公司、北京智游网安科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、中新网络信息安全股份有限公司、河南信安世纪科技有限公司、四川博全科技有限公司、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、张家港欹盾信息技术有限公司、北京明朝万达科技股份有限公司（安元实验室）、北京长亭科技有限公司、山西云助力科技有限公司、上海纽盾科技股份有限公司、上海银基信息安全技术股份有限公司及其他个人白帽子向 CNVD 提交了 1267 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 580 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
360 网神（补天平台）	464	464
北京知道创宇信息技术有限公司	305	304
哈尔滨安天科技股份有限公司	232	0
蓝盾信息安全技术有限公司	204	0
新华三技术有限公司	167	0
北京天融信网络安全技术有限公司	152	13
华为技术有限公司	127	0
漏洞盒子	116	116
北京数字观星科技有限公司	96	0
深圳市深信服电子科技有限公司	84	0
中国电信集团系统集成有限责任公司	83	1
北京神州绿盟科技有限公司	78	0
恒安嘉新(北京)科技股份公司	63	0
北京启明星辰信息安全技术有限公司	55	0
北京无声信息技术有限公司	17	3
杭州安恒信息技术有限公司	3	3
西安四叶草信息技术有限公司	1	1
山东云天安全技术有限公司	79	79
北京圣博润高新技术股份有限公司	74	74
南京联成科技发展股份有限公司	16	16

任子行网络技术股份有限公司	14	14
北京智游网安科技有限公司	11	11
远江盛邦（北京）网络安全科技股份有限公司	10	10
中新网络信息安全股份有限公司	10	10
河南信安世纪科技有限公司	4	4
四川博全科技有限公司	2	2
四川虹微技术有限公司（子午攻防实验室）	2	2
山石网科通信技术有限公司	1	1
张家港款盾信息技术有限公司	1	1
北京明朝万达科技股份有限公司（安元实验室）	1	1
北京长亭科技有限公司	1	1
山西云助力科技有限公司	1	1
上海纽盾科技股份有限公司	1	1
上海银基信息安全技术股份有限公司	1	1
CNCERT 吉林分中心	4	4
CNCERT 新疆分中心	4	4
CNCERT 天津分中心	2	2
CNCERT 湖南分中心	1	1
CNCERT 陕西分中心	1	1
CNCERT 云南分中心	1	1
个人	120	120
报送总计	2609	1267

本周漏洞按类型和厂商统计

本周，CNVD 收录了 301 个漏洞。应用程序漏洞 174 个，WEB 应用漏洞 58 个，网络设备漏洞 35 个，操作系统漏洞 29 个，安全产品漏洞 5 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	174
WEB 应用漏洞	58
网络设备漏洞	35
操作系统漏洞	29
安全产品漏洞	5

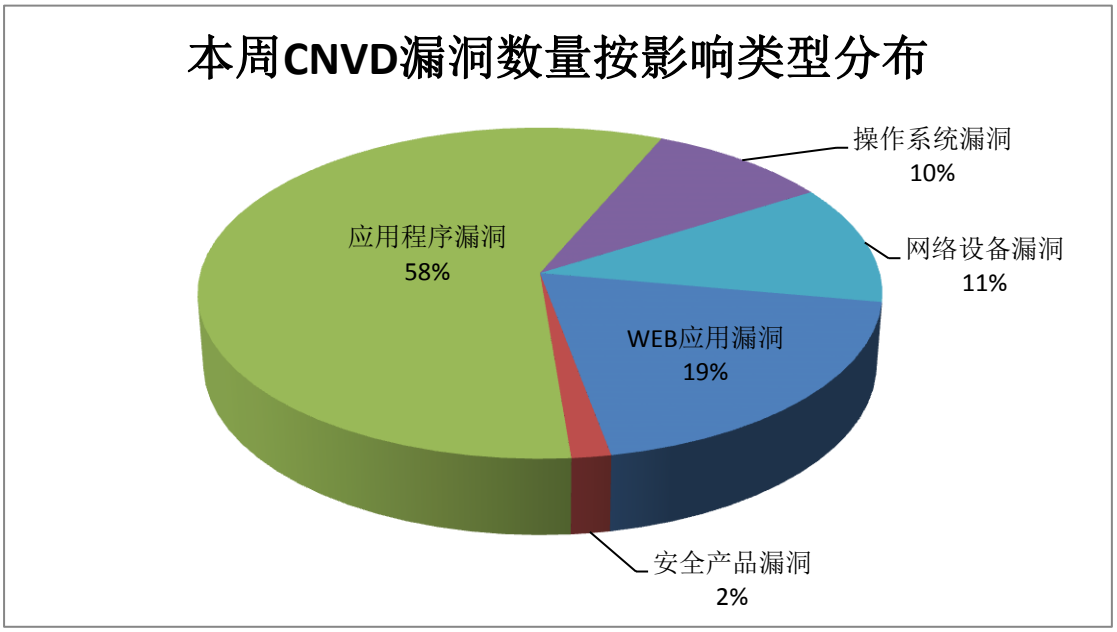

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Cisco、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	Google	32	11%
2	Cisco	27	9%
3	Microsoft	19	6%
4	Adobe	17	6%
5	IBM	8	3%
6	OpenEMR	6	2%

7	Echelon	4	1%
8	Intel	4	1%
9	PHP Scripts Mall	4	1%
10	其他	180	60%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，36 个移动互联网行业漏洞，22 个工控行业漏洞（如下图所示）。其中，“Siemens SCALANCE X Switches 输入验证漏洞、AVEVA InduSoft Web Studio 和 InTouch Machine Edition 缓冲区溢出漏洞、WUZHI CMS SQL 注入漏洞（CNVD-2018-18141）、Google Android System 远程代码执行漏洞（CNVD-2018-18772）、Cisco SD-WAN Solution 权限访问控制漏洞”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/

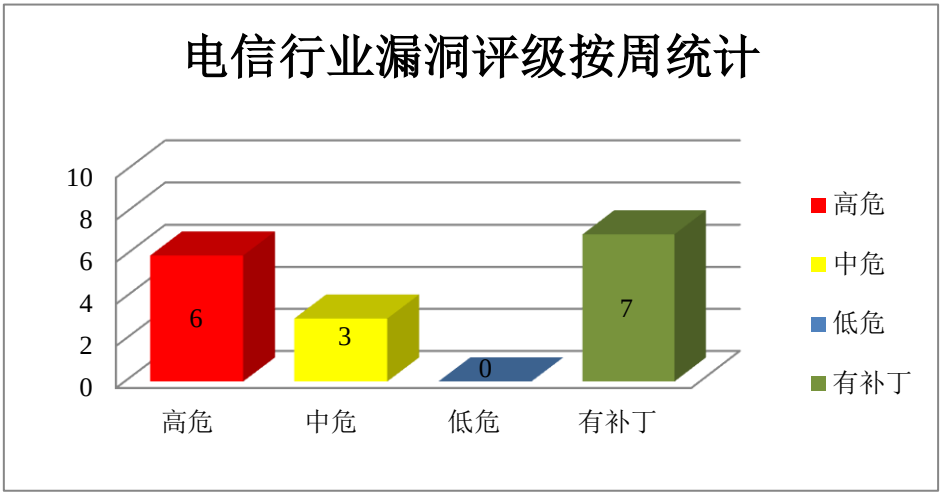

图 3 电信行业漏洞统计

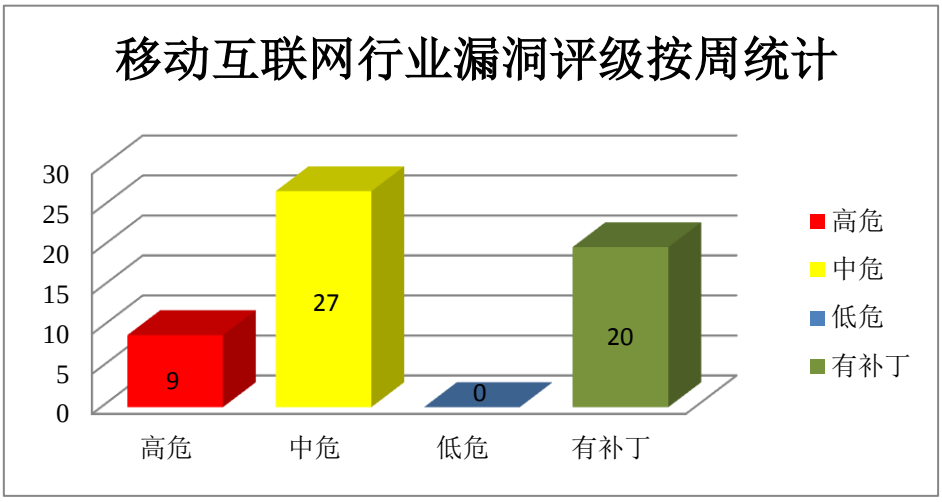

图 4 移动互联网行业漏洞统计

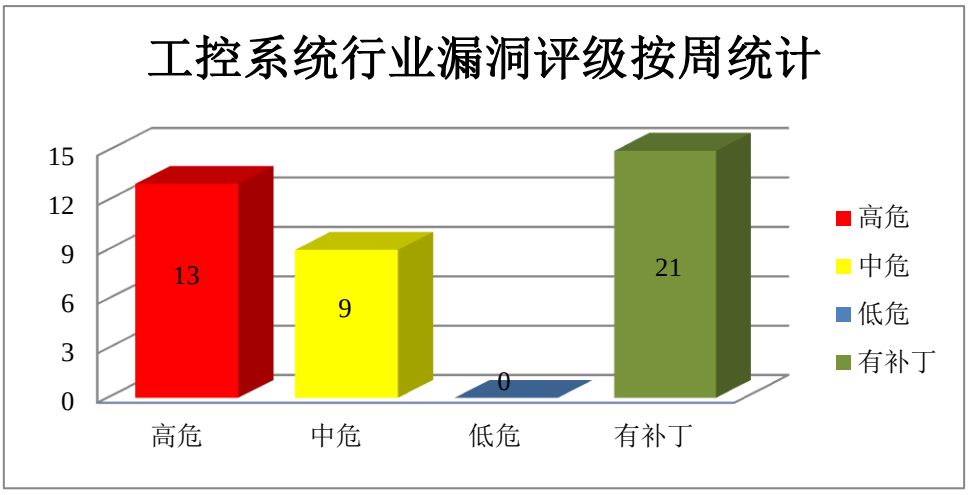

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。Android 是一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、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：Google Chrome SwiftShader 缓冲区溢出漏洞、Google Chrome 请求权限提升漏洞、Google Android Kernel 组件权限提升漏洞（CNVD-2018-18768）、Google Android System 远程代码执行漏洞（CNVD-2018-18772）、Google Android System 权限提升漏洞（CNVD-2018-18773）、Google Android Qualcomm 组件权限提升漏洞（CNVD-2018-18775）、Google Android Framework 权限提升漏洞（CNVD-2018-18779、CNVD-2018-18781）。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-2018-18752
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18764
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18768
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18772
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18773
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18775
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18779
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18781

2、Cisco 产品安全漏洞

Cisco vEdge 100 Series Routers 是一款 100 系列的路由器产品。Cisco Prime Access Registrar 和 Prime Access Registrar Jumpstar 都是访问注册器。Cisco Integrated Management Controller（IMC）Software 是一套用于对 UCS（统一计算系统）进行管理的软件。Cisco Umbrella Enterprise Roaming Client（ERC）是一款防火墙安全客户端。Cisco Enterprise NFV Infrastructure Software（NFVIS）是一套 NVF 基础架构软件平台。Cisco Data Center Network Manager (DCNM)是 Cisco Unified Fabric 的管理系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未授权访问敏感数据，提升权限，执行任意命令，发起拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco SD-WAN Solution 证书验证漏洞、Cisco SD-WAN Solution 命令注入漏洞、Cisco Prime Access Registrar 拒绝服务漏洞、Cisco Integrated Management Controller 命令注入漏洞、Cisco Umbrella Enterprise Roaming Client 输入验证漏洞、Cisco Enterprise NFV Infrastructure Software 输入验证漏洞、Cisco Data Center Network Manager 权限提升漏洞、Cisco SD-WAN Solution 权限访问控制漏洞。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-2018-18789
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18790
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18787
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18795
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18794
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18797
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18796
http://www.cnvd.org.cn/flaw/show/CNVD-2018-18800

3、Microsoft 产品安全漏洞

Microsoft Internet Explorer 是一款流行的 WEB 浏览器。Microsoft Edge 是一款 Web 浏览器。Microsoft SharePoint Enterprise Server 是一套企业业务协作平台。Microsoft Excel 是 Office 套件中的一款电子表格处理软件。Microsoft Word 是 Office 套件中的一款文字处理软件。Microsoft Windows 10、Windows Server 2016、Windows Server 2012 等都是美国微软（Microsoft）公司发布的一系列操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，提升权限，执行任意代码，破坏内存。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 和 Edge 内存破坏漏洞（CNVD-2018-18477）、Microsoft Windows kernel 提权漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2018-18622）、Microsoft Word 远程代码执行漏洞（CNVD-2018-18623）、Microsoft Internet Explorer 和 Edge 内存破坏漏洞（CNVD-2018-18626）、Microsoft Windows Hyper-V 信息泄露漏洞（CNVD-2018-18628）、Microsoft Windows GDI 组件信息泄露漏洞（CNVD-2018-18629）、Microsoft SharePoint Enterprise Server 提权漏洞。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-2018-18477

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18617

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18622

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18623

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18626

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18628

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18629

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18630

4、Adobe 产品安全漏洞

Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Adobe Reader 是一套 PDF 文档阅读软件。Adobe Flash Player 是一款跨平台、基于浏览器的多媒体播放器产品。Adobe Flash Player 是一款跨平台、基于浏览器的多媒体播放器产品。Adobe ColdFusion 是一款动态 Web 服务器产品，其运行的 CFML（ColdFusion Markup Language）是针对 Web 应用的一种程序设计语言。本周，该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，执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 任意代码执行漏洞（CNVD-2018-18449、CNVD-2018-18450）、Adobe Flash Player 权限提升漏洞（CNVD-2018-18451）、Adobe Flash Player 信息泄露漏洞（CNVD-2018-18481）、Adobe ColdFusion 任意代码执行漏洞、Adobe ColdFusion 任意文件重写漏洞、Adobe ColdFusion 任意文件上传漏洞、Adobe ColdFusion 不可信数据反序列化漏洞（CNVD-2018-18735）。上述漏洞的综合评级为“高危”。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-2018-18449

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18450

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18451

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18481

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18734

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18732

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18733

http://www.cnvd.org.cn/flaw/show/CNVD-2018-18735

5、Red Hat spice-client 缓冲区溢出漏洞

Red Hat SPICE 是一个企业虚拟化桌面版所使用的自适应远程呈现开源协议，它主要用于将用户与其虚拟桌面进行连接，能够提供与物理桌面完全相同的最终用户体验。spice-client 是它的客户端程序。本周，Red Hat spice-client 被披露存在缓冲区溢出漏洞。攻击者可借助恶意的服务器利用该漏洞造成客户端崩溃或执行任意代码。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-2018-18621

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-2018-18306	多款 Echelon 产品信息泄露漏洞（CNVD-2018-18306）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.echelon.com/software-downloads?ele=153-0608-01A
CNVD-2018-18479	IBM WebSphere Application Server 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://www.ibm.com/support/docview.wss?uid=swg22016254
CNVD-2018-18592	多款 Echelon 产品信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.echelon.com/software-downloads?ele=153-0608-01A
CNVD-2018-18613	SIMATIC WinCC OA 权限提升漏洞	高	西门子已经确定了以下具体的解决方法和缓解措施：https://portal.etm.at/patchdownload.php?fp=version_3.14/win64vc12/ReadmeP021.txt https://portal.etm.at/index.php?option=c

			om_phocadownload&view=category&id=52:security&Itemid=81
CNVD-2018-18612	Siemens SCALANCE X Switches 输入验证漏洞	高	用户可联系供应商获得补丁信息：https://support.industry.siemens.com/cs/us/en/view/109753720
CNVD-2018-18619	Ansible Tower 权限访问控制漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://docs.ansible.com/ansible-tower/3.0.3/html/upgrade-migration-guide/release_notes.html
CNVD-2018-18784	Apache Syncope 远程代码执行漏洞（CNVD-2018-18784）	高	用户可联系供应商获得补丁信息：https://syncope.apache.org/security
CNVD-2018-18801	Dell EMC ECOM XML 外部实体注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.dell.com/zh-cn
CNVD-2018-18891	e107 SQL 注入漏洞（CNVD-2018-18891）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/e107inc/e107/commit/ec483e9379aa622bfcc1b853b189c74288771f27
CNVD-2018-18893	ZOHO ManageEngine Desktop Central 权限提升漏洞（CNVD-2018-18893）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.manageengine.com/products/desktop-central/elevation-of-system-privilege.html

小结：本周，Google 被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或发起拒绝服务攻击。此外，Cisco、Microsoft、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞未授权访问敏感数据，提升权限，执行任意命令，破坏内存，发起拒绝服务等。另外，Red Hat spice-client 被披露存在缓冲区溢出漏洞。攻击者可借助恶意的服务器利用该漏洞造成客户端崩溃或执行任意代码。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、Netgate Registry Clenaner 本地权限提升漏洞

验证描述

NETGATE Registry Cleaner 是一个磁盘清理软件。

Netgate Registry Clenaner 存在本地权限提升漏洞，攻击者可利用漏洞提升权限。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=30846

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-18308

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. 通过 Safari 浏览器漏洞进行的 URL 欺骗攻击

近日，国外安全专家发现了一个严重漏洞（CVE-2018-8383），允许攻击者在 Windows 的 Edge 浏览器和 iOS 的 Safari 中进行 URL 欺骗攻击。微软上个月的安全更新已经修复了 Edge 地址栏欺骗漏洞，但 Safari 尚未修复，可能使 Apple 用户受到网络钓鱼攻击。据悉，该漏洞可能允许攻击者利用 JS 加载页面，导致页面地址显示在 URL 栏中，然后用恶意代码替换网页中的代码。

参考链接：https://thehackernews.com/2018/09/browser-address-spoofing-vulnerability.html

2. Intel CSME 漏洞预警

在英特尔 CSME，英特尔服务器平台服务和英特尔可信执行引擎固件中潜在的安全漏洞会允许信息泄漏，英特尔正在发布英特尔 CSME，英特尔服务器平台服务和英特尔可信执行引擎更新，以缓解此潜在漏洞。漏洞存在于 11.21.55 版本之前的英特尔 CSME 中的子系统，4.0 版本之前的英特尔服务器平台服务和 3.1.55 版本之前的英特尔可信执行引擎固件中，可能允许未经身份验证的用户通过物理访问来修改或泄漏信息。

参考链接：https://www.anquanke.com/post/id/159597

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