国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 8 月 27 日-2018 年 9 月 2 日　　**2018 年第 35 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 356 个，其中高危漏洞 127 个、中危漏洞 205 个、低危漏洞 24 个。漏洞平均分值为 6.20。本周收录的漏洞中，涉及 0day 漏洞 132 个（占 37%），其中互联网上出现“QNAP Q'center Virtual Appliance 命令注入漏洞、TP-Link WR840N 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 879 个，与上周（986 个）环比下降 11%。

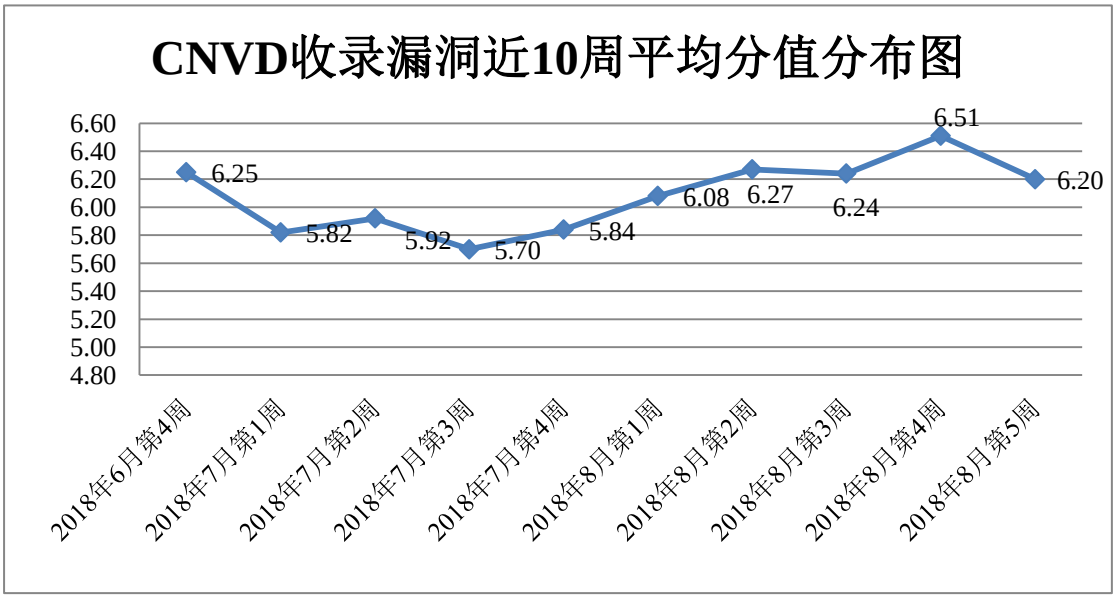

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、北京知道创宇信息技术有限公司、北京启明星辰信息安全技术有限公司、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、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、北京国舜科技股份有限公司、北京明朝万达科技股份有限公司（安元实验室）、中新网络信息安全股份有限公司、四川虹微技术有限公司（子午攻防实验室）、任子行网络技术股份有限公司、北京长亭科技有限公司、山石网科通信技术有限公司、河南信安世纪科技有限公司、上海纽盾科技股份有限公司及其他个人白帽子向 CNVD 提交了 879 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 295 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	357	9
北京知道创宇信息技术有限公司	319	315
北京启明星辰信息安全技术有限公司	319	1
哈尔滨安天科技股份有限公司	194	0
360 网神（补天平台）	193	193
新华三技术有限公司	122	0
华为技术有限公司	117	0
漏洞盒子	102	102
北京神州绿盟科技有限公司	68	0
中国电信集团系统集成有限责任公司	68	0
恒安嘉新(北京)科技股份公司	53	0
深圳市深信服电子科技有限公司	27	0
北京无声信息技术有限公司	17	12
上海银基信息安全技术股份有限公司	31	31
厦门服云信息科技有限公司	4	0

山东云天安全技术有限公司	24	24
南京联成科技发展股份有限公司	17	17
上海谋乐网络科技有限公司	9	9
北京国舜科技股份有限公司	5	5
北京明朝万达科技股份有限公司（安元实验室）	5	5
中新网络信息安全股份有限公司	5	5
四川虹微技术有限公司（子午攻防实验室）	4	4
任子行网络技术股份有限公司	3	3
北京长亭科技有限公司	1	1
山石网科通信技术有限公司	1	1
河南信安世纪科技有限公司	1	1
上海纽盾科技股份有限公司	1	1
CNCERT 山西分中心	24	24
CNCERT 天津分中心	5	5
CNCERT 新疆分中心	4	4
CNCERT 四川分中心	4	4
CNCERT 河北分中心	4	4
CNCERT 广东分中心	3	3
CNCERT 吉林分中心	2	2
CNCERT 海南分中心	1	1
CNCERT 贵州分中心	1	1
CNCERT 上海分中心	1	1
个人	91	91

报送总计	2207	879

本周漏洞按类型和厂商统计

本周，CNVD 收录了 356 个漏洞。应用程序漏洞 195 个，网络设备漏洞 58 个，WEB 应用漏洞 50 个，操作系统漏洞 45 个，安全产品漏洞 7 个，数据库漏洞 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
应用程序漏洞	195
网络设备漏洞	58
WEB 应用漏洞	50
操作系统漏洞	45
安全产品漏洞	7
数据库漏洞	1

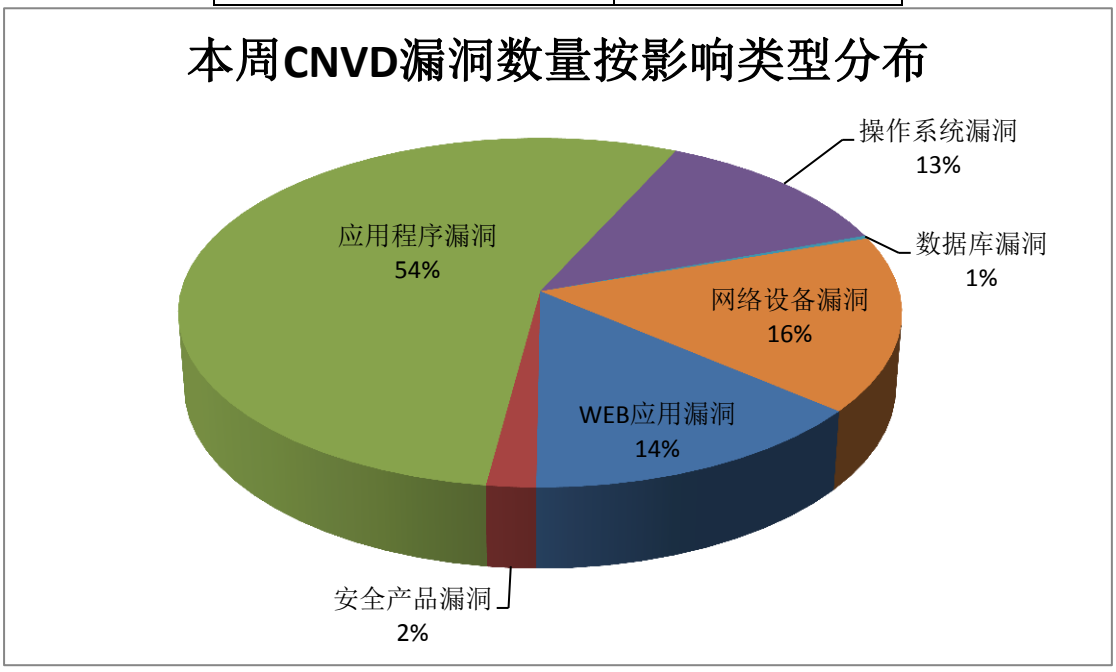

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、IBM 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	34	10%
2	Microsoft	25	7%
3	IBM	19	5%

4	Samsung	13	4%
5	Linux	8	2%
6	Drupal	6	2%
7	INSTEON	6	2%
8	OpenEMR	6	2%
9	Kraftway	5	1%
10	其他	234	65%

本周行业漏洞收录情况

本周，CNVD 收录了 31 个电信行业漏洞，18 个移动互联网行业漏洞，1 个工控行业漏洞（如下图所示）。其中，“多款 Huawei 产品插件签名绕过漏洞、Google Android Framework 远程代码执行漏洞、Mikrotik RouterOS 栈缓冲区溢出漏洞、Trihedral Engineering Limited VTScada ICSA-17-304-0 存在多个漏洞、Cisco Data Center Network Manager 目录遍历漏洞”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/

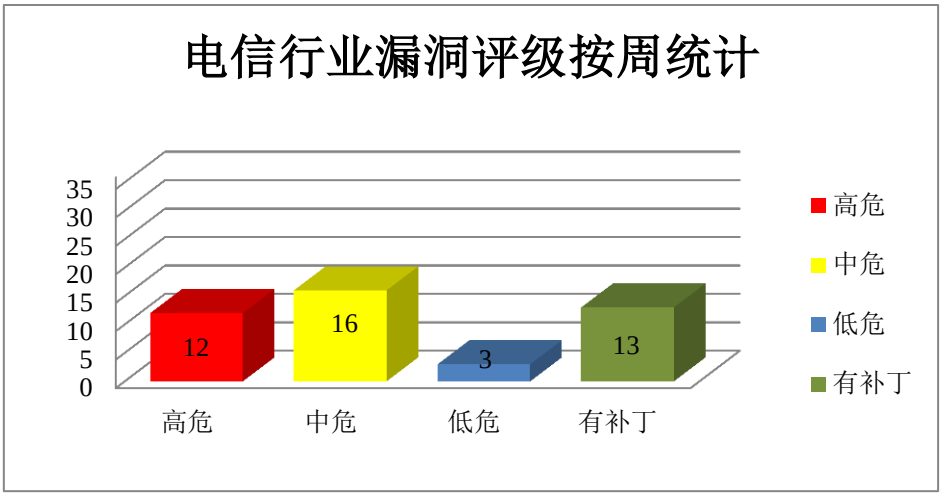

图 3 电信行业漏洞统计

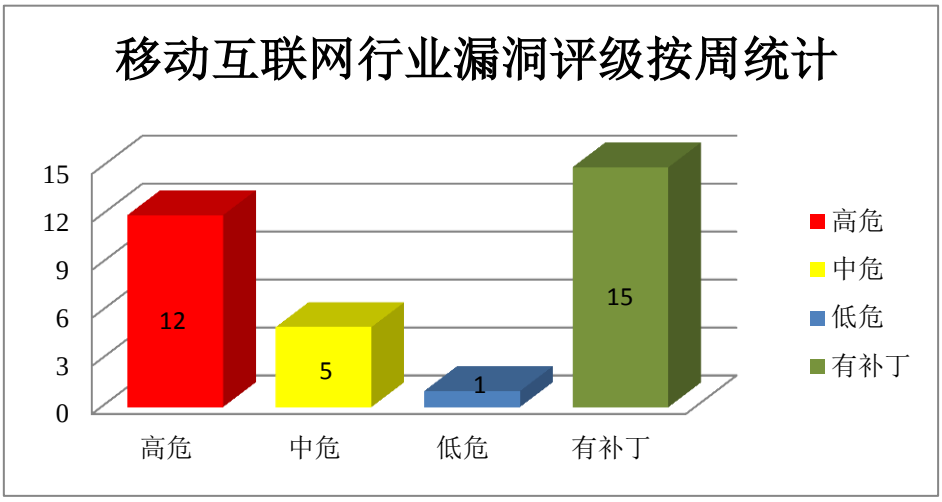

图 4 移动互联网行业漏洞统计

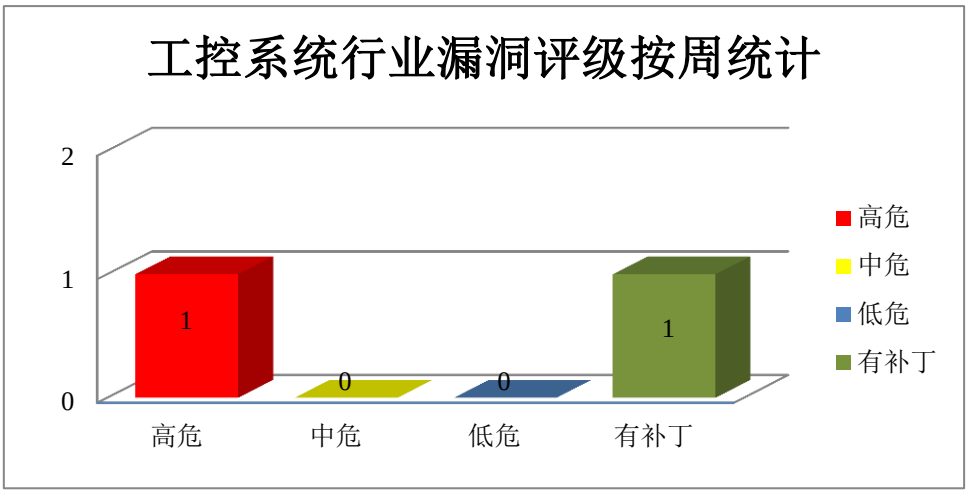

图 5 工控系统行业漏洞统计

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，攻击者可利用漏洞获取敏感信息，权限提升，执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Kernel 组件权限提升漏洞（CNVD-2018-16973、CNVD-2018-16972）、Google Android System 权限提升漏洞（CNVD-2018-16976）、Google Android Media framework 权限提升漏洞（CNVD-2018-16981）、Google Android Framework 信息泄露漏洞（CNVD-2018-16983）、Google Chrome 堆缓冲区溢出漏洞（CNVD-2018-17041、CNVD-2018-17043、CNVD-2018-17049）。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-2018-16973

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16972

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16976

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16981

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16983

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17041

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17043

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17049

2、Microsoft 产品安全漏洞

Microsoft Windows 10 是一套个人电脑使用的操作系统。Windows Server 2008 SP 2 是一套服务器操作系统。Windows Server Version 1709 是一套服务器操作系统。Windows PDF Library 是其中的一个 PDF 库。Microsoft Excel 是一款电子表格处理软件。Internet Explorer 是一款网页浏览器。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：Microsoft Windows LNK 远程代码执行漏洞（CNVD-2018-16833、CNVD-2018-16832）、Microsoft Windows Graphics Component 远程执行代码漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2018-16841）、Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2018-16846）、Microsoft Windows Shell 远程代码执行漏洞（CNVD-2018-17078）、Microsoft Windows PDF 远程代码执行漏洞（CNVD-2018-17083）、Microsoft Excel 远程代码执行漏洞（CNVD-2018-17092）。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-2018-16833

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16832

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16840

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16841

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16846

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17078

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17083

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17092

3、Samsung 产品安全漏洞

Samsung SmartThings Hub 是一款智能家居管理设备。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或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Samsung SmartThings Hub 缓冲区溢出漏洞、Samsu

ng SmartThings Hub video-core HTTP 服务器缓冲区溢出漏洞（CNVD-2018-17077、CNVD-2018-17076、CNVD-2018-17075）、Samsung SmartThings Hub 栈缓冲区溢出漏洞、Samsung SmartThings Hub video-core HTTP 服务器注入漏洞、Samsung SmartThings Hub HTTP 响应拆分漏洞、Samsung SmartThings Hub video-core HTTP 服务器覆盖漏洞。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-2018-17069

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17077

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17076

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17075

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17074

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17079

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17081

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17151

4、IBM 产品安全漏洞

IBM API Connect（又名 APIConnect）是一套用于管理 API 生命周期的集成解决方案。IBM WebSphere Application Server（WAS）是一款应用服务器产品，它是 Java EE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。IBM InfoSphere Information Server 是信息集成平台。IBM Security Identity Manager（ISIM）是一套身份管理和治理解决方案。IBM Spectrum Scale 是一套基于 IBM GPFS（专为 PB 级存储管理而优化的企业文件管理系统）的可扩展的数据及文件管理解决方案。GSKit 是其中的一套 IBM 产品的安全管理工具。IBM Netezza Platform Software 是一套基于 InfoSphere Smart Analytics 技术并可应对实时决策、欺诈检测等需求的集成数据系统。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞诱使服务器执行恶意的调用，获取敏感信息，提升权限，执行任务代码。

CNVD 收录的相关漏洞包括：IBM API Connect 服务器端请求伪造漏洞、IBM WebSphere Application Server 信息泄露漏洞（CNVD-2018-16971）、IBM WebSphere Application Server Liberty 信息泄露漏洞（CNVD-2018-17070）、IBM Maximo Asset Management SQL 注入漏洞（CNVD-2018-17089）、IBM InfoSphere Information Server 信息泄露漏洞（CNVD-2018-17156）、IBM Security Identity Manager Virtual Appliance 代码执行漏洞、IBM Spectrum Scale GSKit 提权漏洞、IBM Netezza Platform Software 本地权限提升漏洞。其中，“IBM API Connect 服务器端请求伪造漏洞、IBM Netezza Platform Software 本地权限提升漏洞”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-2018-16969

http://www.cnvd.org.cn/flaw/show/CNVD-2018-16971

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17070

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17089

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17156

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17154

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17159

http://www.cnvd.org.cn/flaw/show/CNVD-2018-17160

5、ASUS DSL-N12E_C1 远程命令执行漏洞

ASUS DSL-N12E_C1 是华硕（ASUS）公司的一款无线路由器产品。本周，ASUS DSL-N12E_C1 被披露存在远程命令执行漏洞。远程攻击者可借助服务参数利用该漏洞执行任意操作系统命令。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-2018-17193

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-2018-16272	Splunk 存在多个本地提权漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.splunk.com/view/SP-CAAAP3M
CNVD-2018-16278	Trovebox PHP 身份验证绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/photo/frontend
CNVD-2018-16280	HPE Integrated Lights Out（iLO）越权漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03844en_us
CNVD-2018-16523	Mikrotik RouterOS 栈缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://mikrotik.com/download/changelogs；https://mikrotik.com/download/changelogs/bugfix-release-tree
CNVD-2018-16536	多款 Huawei 产品插件签名绕过漏洞	高	华为已发布版本修复该漏洞。安全预警链接：http://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20180827-01-gateway-cn

CNVD-2018-16693	Linux kerne 'uvesafb_setcmap' 函数 l 整数溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/torvalds/linux/commit/9f645bcc566a1e9f921bdae7528a01ced5bc3713
CNVD-2018-16702	Cisco Data Center Network Manager 目录遍历漏洞	高	思科已发布了软件更新，请联系厂商下载更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180828-dcnm-traversal
CNVD-2018-16703	Adobe Creative Cloud Desktop Application 权限提升漏洞	高	用户可联系供应商获得补丁信息：https://helpx.adobe.com/security/products/creative-cloud/apsb18-32.html
CNVD-2018-16949	phpMyFAQ SQL 注入漏洞（CNVD-2018-16949）	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.phpmyfaq.de/security/advisory-2014-09-16
CNVD-2018-17065	Red Hat OpenShift Container Platform source-to-image component 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://access.redhat.com/errata/RHSA-2018:2013

小结：本周，Google 被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，权限提升，执行任意代码。此外，Microsoft、Samsung、IBM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞诱使服务器执行恶意的调用，获取敏感信息，提升权限，执行任务代码或发起拒绝服务攻击。另外，ASUS DSL-N12E_C1 被披露存在远程命令执行漏洞。远程攻击者可借助服务参数利用该漏洞执行任意操作系统命令。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. ECShop 全系列版本远程代码执行高危漏洞

ECShop 全系列版本存在远程代码执行漏洞。该漏洞产生的根本原因在于 ECShop 系统的 user.php 文件中，display 函数的模板变量可控，导致注入，配合注入可达到远程代码执行的效果。使得攻击者无需登录等操作，直接可以获得服务器的权限。

参考链接：http://www.freebuf.com/vuls/182899.html

2. 医疗网关和设备受老旧的“厄运 Cookie”漏洞威胁

近日，热门医疗网关设备 Qualcomm Life Capsule Datacaptor Terminal Server（DTS）常被医院用来将医疗设备连接到更大的数字网络基础设施，该网关常用于连接显示器、呼吸机、麻醉输送系统和输液泵等。据披露，DTS 与其他许多物联网设备一样，具有用于配置的 Web 管理接口，该接口使用了名为“RomPager”的软件组件，而 DTS

使用的 RomPager 版本易受到“厄运 Cookie”（CVE-2014-9222）影响，可被攻击者利用执行未经授权的代码，获得设备的管理员权限。

参考链接：https://www.easyaq.com/news/956265357.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