国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 5 月 21 日-2018 年 5 月 27 日 **2018 年第 21 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 335 个，其中高危漏洞 115 个、中危漏洞 209 个、低危漏洞 11 个。漏洞平均分值为 6.32。本周收录的漏洞中，涉及 0day 漏洞 56 个（占 17%），其中互联网上出现“Digital Guardian Management Console 远程代码执行漏洞、EFS Easy File Sharing Web Server 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 458 个，与上周（540 个）环比下降 15%。

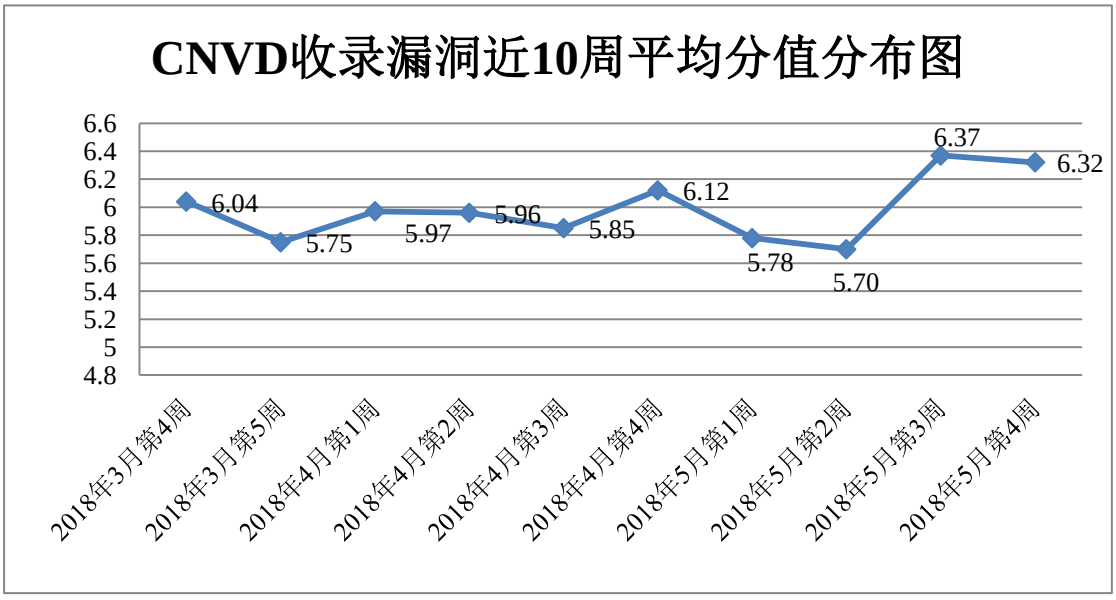

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，蓝盾信息安全技术有限公司、阿里云计算有限公司、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、华为技术有限公

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、四川虹微技术有限公司（子午攻防实验室）、中新网络信息安全股份有限公司、中国科学院信息工程研究所、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 458 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 296 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
蓝盾信息安全技术有限公司	1207	0
阿里云计算有限公司	478	0
北京天融信网络安全技术有限公司	411	2
哈尔滨安天科技股份有限公司	218	0
360 网神（补天平台）	162	162
华为技术有限公司	155	1
北京启明星辰信息安全技术有限公司	150	3
漏洞盒子	134	134
新华三技术有限公司	114	0
北京数字观星科技有限公司	100	0
中国电信集团系统集成有限责任公司	51	0
恒安嘉新(北京)科技股份公司	44	0
北京神州绿盟科技有限公司	44	0
厦门服云信息科技有限公司	21	1
北京无声信息技术有限公司	11	0
北京知道创宇信息技术有限公司	2	1
南京联成科技发展股份有限公司	9	9

四川虹微技术有限公司（子午攻防实验室）	7	7
中新网络信息安全股份有限公司	4	4
中国科学院信息工程研究所	2	2
任子行网络技术股份有限公司	1	1
CNCERT 山西分中心	15	15
CNCERT 吉林分中心	5	5
CNCERT 宁夏分中心	4	4
CNCERT 广东分中心	3	3
CNCERT 贵州分中心	1	1
CNCERT 上海分中心	1	1
个人	102	102
报送总计	3456	458

本周漏洞按类型和厂商统计

本周，CNVD 收录了 335 个漏洞。其中应用程序漏洞 208 个，操作系统漏洞 64 个，WEB 应用漏洞 30 个，网络设备漏洞 30 个，安全产品漏洞 3 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	208
操作系统漏洞	64
WEB 应用漏洞	30
网络设备漏洞	30
安全产品漏洞	3

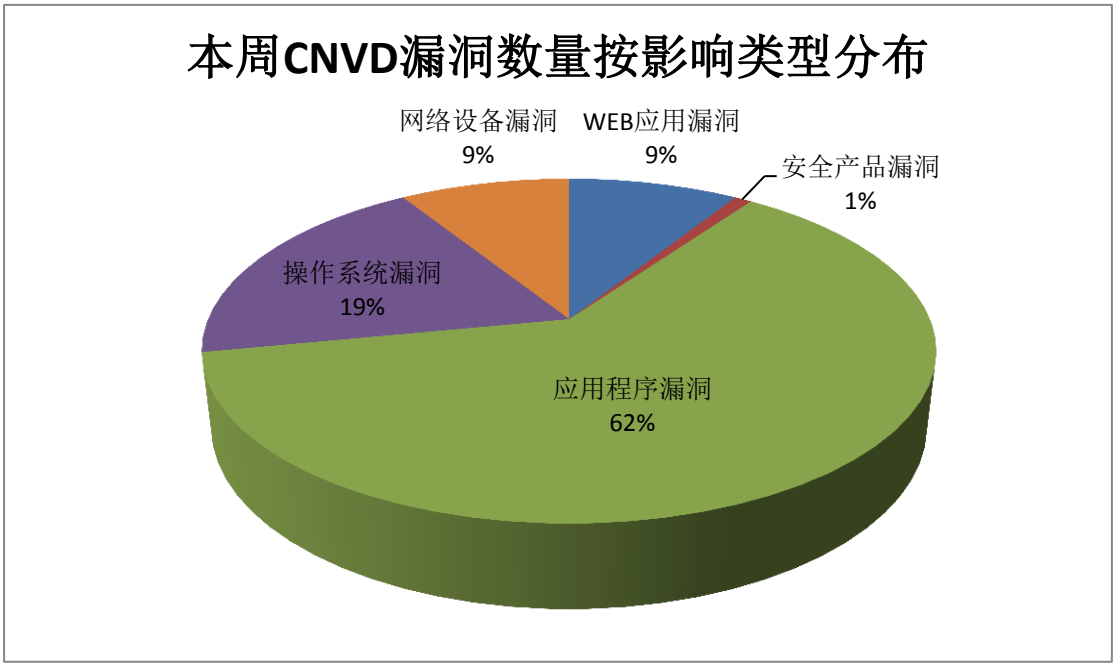

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Foxit、Google、Mozilla 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	Foxit	53	16%
2	Google	34	10%
3	Mozilla	14	4%
4	Apple	14	4%
5	Microsoft	10	3%
6	F5	9	3%
7	Apache	6	2%
8	Linux	6	2%
9	IBM	5	1%
10	其他	184	55%

本周行业漏洞收录情况

本周，CNVD 收录了 13 个电信行业漏洞，52 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“Belkin N750 栈缓冲区溢出漏洞、Phoenix Contact managed FL SWITCH 命令注入漏洞、Apple iOS Telephony 缓冲区溢出漏洞、Google Android 缓冲

区溢出漏洞（CNVD-2018-10124）、Google Android 安全绕过漏洞”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/

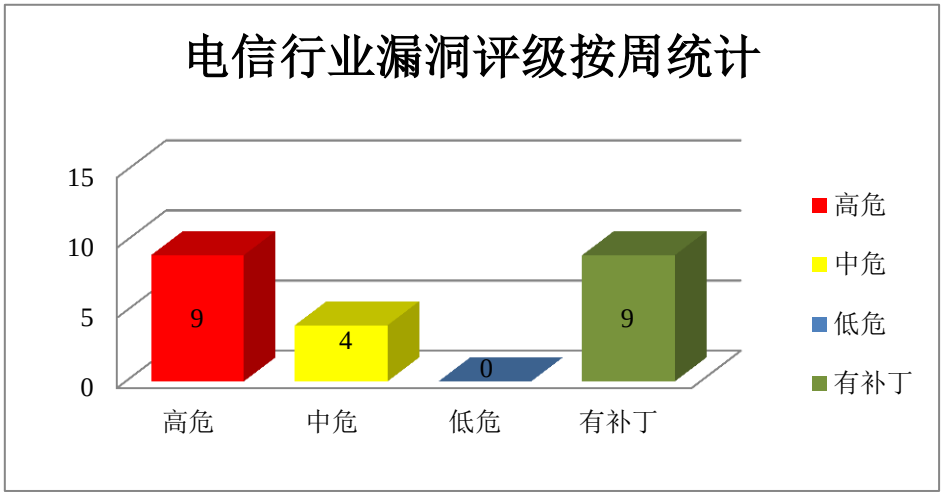

图 3 电信行业漏洞统计

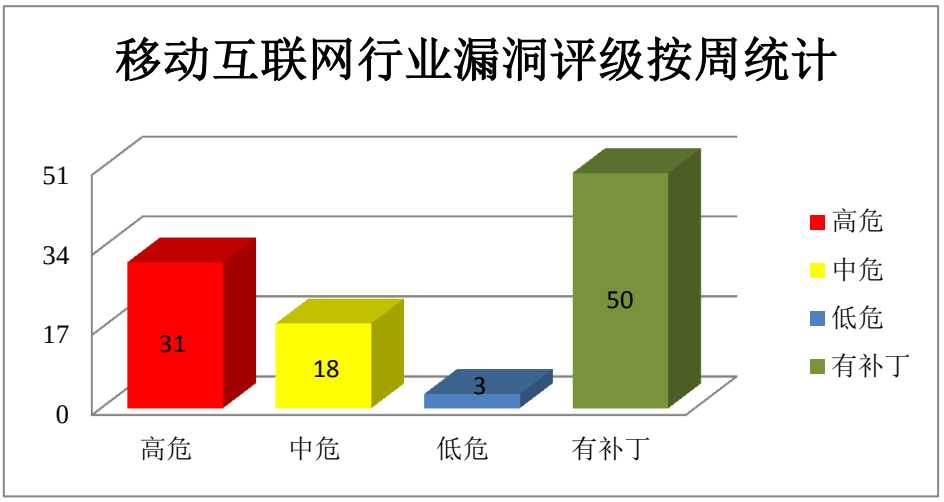

图 4 移动互联网行业漏洞统计

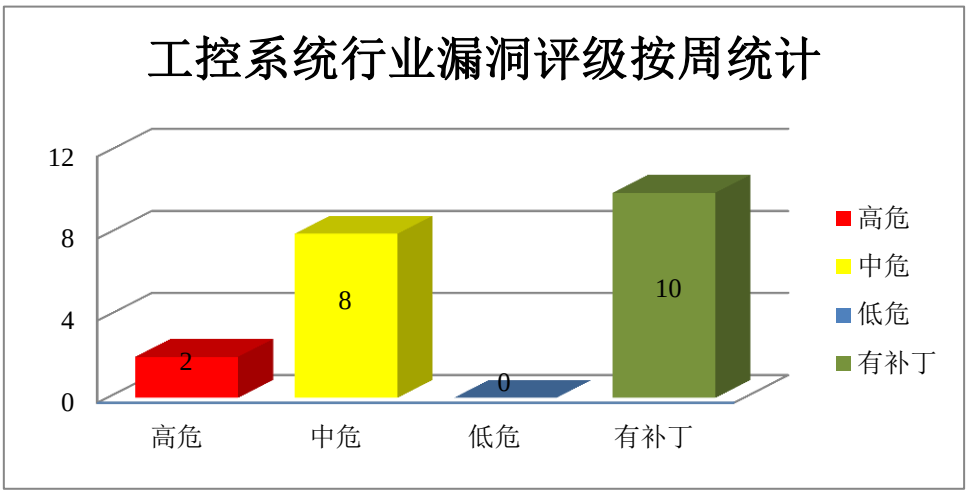

图 5 工控行业漏洞统计

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

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。DRM API 是其中的一个数字版权管理 API（应用程序接口）。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、执行任意代码或绕过安全限制等。

CNVD 收录的相关漏洞包括：Google Android 缓冲区溢出漏洞（CNVD-2018-10124）、Google Android 缓冲区越边界读取漏洞（CNVD-2018-10035、CNVD-2018-10042）、Google Android 内存错误引用漏洞（CNVD-2018-10125）、Google Android 权限提升漏洞（CNVD-2018-10119）、Google Android 远程代码执行漏洞（CNVD-2018-10120）、Google Android DRM API 缓冲区越边界读取漏洞、Google Android 安全绕过漏洞，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-2018-10124

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10035

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10042

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10125

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10119

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10120

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10069

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09893

2、Microsoft 产品安全漏洞

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。Edge 是其中的一个系统附带的默认浏览器。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 ChakraCore 和 Edge 远程代码执行漏洞（CNVD-2018-10201、CNVD-2018-10202、CNVD-2018-10204、CNVD-2018-10205、CNVD-2018-10206、CNVD-2018-10207、CNVD-2018-10208、CNVD-2018-10210）。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-2018-10201

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10202

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10204

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10205

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10206

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10207

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10208

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10210

3、Apple 产品安全漏洞

Apple Safari 是美国苹果公司的一款 Web 浏览器，Apple iOS 是为移动设备所开发的一套操作系统；macOS High Sierra 是一套专为 Mac 计算机所开发的专用操作系统。Apple iOS 是美国苹果（Apple）公司为移动设备所开发的一套操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Apple iOS Safari 欺骗漏洞、Apple iOS 和 macOS High Sierra Mail 中间人攻击漏洞、Apple iOS 和 macOS High Sierra PluginKit 竞争条件漏洞、Apple Safari WebKit 内存破坏漏洞（CNVD-2018-09990）、Apple Safari 任意代码执行漏洞（CNVD-2018-09989）、Apple iOS Telephony 缓冲区溢出漏洞、Apple iOS Telephony 拒绝服务漏洞、多款 Apple 产品 Quick Look 竞争条件漏洞。除“Apple iOS Safari 欺骗漏洞、Apple iOS 和 macOS High Sierra Mail 中间人攻击漏洞”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-2018-09967

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09977

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09974

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09990

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09989

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09971

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09970

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09975

4、Mozilla 产品安全漏洞

Mozilla Firefox 浏览器（火狐）是一个自由的、开放源码的浏览器，适用于 Windows、Linux 及 MacOSX 平台。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Mozilla Firefox JavaScript 注入漏洞、Mozilla Firefox XSLT 缓冲区溢出漏洞、Mozilla Firefox 堆内存错误引用漏洞、Mozilla Firefox 同源保护绕过漏洞、Mozilla Firefox 未初始化内存使用漏洞、Mozilla Firefox 整数溢出漏洞（CNVD-2018-10242）、Mozilla Firefox 内存错误引用漏洞（CNVD-2018-10245、CNV

D-2018-10246）。除“Mozilla Firefox JavaScript 注入漏洞、Mozilla Firefox XSLT 缓冲区溢出漏洞、Mozilla Firefox 堆内存错误引用漏洞”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-2018-10243

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10234

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10233

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10244

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10241

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10242

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10245

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10246

5、D-Link DIR-550A 和 DIR-604M 权限获取漏洞

D-Link DIR-550A 和 DIR-604M 都是友讯（D-Link）公司的无线路由器产品。本周，D-Link 被披露存在权限获取漏洞，攻击者可通过使用默认的 TELNET 账户利用该漏洞获取访问权限。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-2018-10000

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-2018-10002	GE 多款 PACSystems 产品输入验证错误漏洞	高	用户可联系供应商获得补丁信息：https://digitalsupport.ge.com
CNVD-2018-10059	GNU C Library 任意代码执行漏洞	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.gnu.org/software/libc/
CNVD-2018-10151	Phoenix Contact managed FL SWITCH 命令注入漏洞	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.phoenixcontact.com/
CNVD-2018-10149	Phoenix Contact managed FL SWITCH 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.phoenixcontact.com/
CNVD-2018-10156	tinysvcmdns library 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://bitbucket.org/geekman/tinysvcmdns
CNVD-2018-10216	Foxit Reader 任意代码执行漏洞（CNVD-2018-10216）	高	厂商已发布漏洞修复程序，请及时关注更新：

			https://www.foxitsoftware.com/support/security-bulletins.php
CNVD-2018-10303	HP SiteScope 未指明未经授权访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.auscert.org.au/bulletins/52758/
CNVD-2018-10332	procps-ng 权限提升漏洞	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://gitlab.com/procps-ng/procps
CNVD-2018-10334	procps-ng 整数溢出漏洞	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://gitlab.com/procps-ng/procps
CNVD-2018-10333	procps-ng 任意代码执行漏洞	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://gitlab.com/procps-ng/procps

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、执行任意代码或绕过安全限制等。此外，Microsoft、Apple、Mozilla 等多款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、提升权限或发起拒绝服务攻击。另外，D-Link 被披露存在权限获取漏洞，攻击者可通过使用默认的 TELNET 账户利用该漏洞获取访问权限。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. RTU 曝 10 分漏洞，欧盟能源企业或面临大范围 DoS 攻击

来自拉脱维亚安全厂商 CERT.LV 公司的两名研究人员 Bernhards Blumbergs 与 Arturs Danilevics 最新发现，由爱沙尼亚 Martem 公司制造的 Telem-GW6 与 Telem-GWM 产品中存在安全漏洞，可被用于实施拒绝服务（简称 DoS）攻击并执行任意代码及命令。这些存在安全漏洞的产品属于数据集中器，负责收集变电站外围设备的相关数据。其中最严重的安全漏洞 CVE-2018-10603（CVSS 评分：10 分满分），其允许网络上的恶意节点发送未经授权的命令并控制工业流程。另一项高危漏洞 CVE-2018-10607，属于不受控类资源消耗问题。根据 ICS-CERT 方面的解释，攻击者能够建立一条或者多条面向输入/输出附件（简称 IOA）的新连接并以非正常方式将其关闭，从而在工业流程控制通道内引发 DoS 状况

参考链接：https://www.easyaq.com/news/1763244545.shtml

2. 54 个国家大量路由器被僵尸网络 VPNFilter 控制

思科和赛门铁克公司于美国时间 2018 年 5 月 23 日陆续发出安全预警：黑客利用一个复杂的规模化恶意软件 VPNFilter，感染了全球 54 个国家的 50 万台路由器，并构建

了庞大的僵尸网络，Linksys，MikroTik，Netgear 和 TP-Link 等多家路由器设备厂商受影响。思科称在逾 50 万台路由器上发现了 VPNFilter 恶意软件，全球 54 个国家，多个品牌的路由器遭遇感染。思科表示，攻击者未使用 0Day 漏洞构建该僵尸网络，而是利用的老旧的公开已知漏洞感染路由器。

参考链接：https://www.easyaq.com/news/1100964515.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