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 14 日-2018 年 5 月 20 日 **2018 年第 20 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 353 个，其中高危漏洞 149 个、中危漏洞 189 个、低危漏洞 15 个。漏洞平均分值为 6.37。本周收录的漏洞中，涉及 0day 漏洞 83 个（占 24%），其中互联网上出现“Nagios XI admin/commandline.php SQL 注入漏洞、Foscam C1 Indoor HD Camera 固件恢复未签名图像漏洞”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 540 个，与上周（614 个）环比下降 12%。

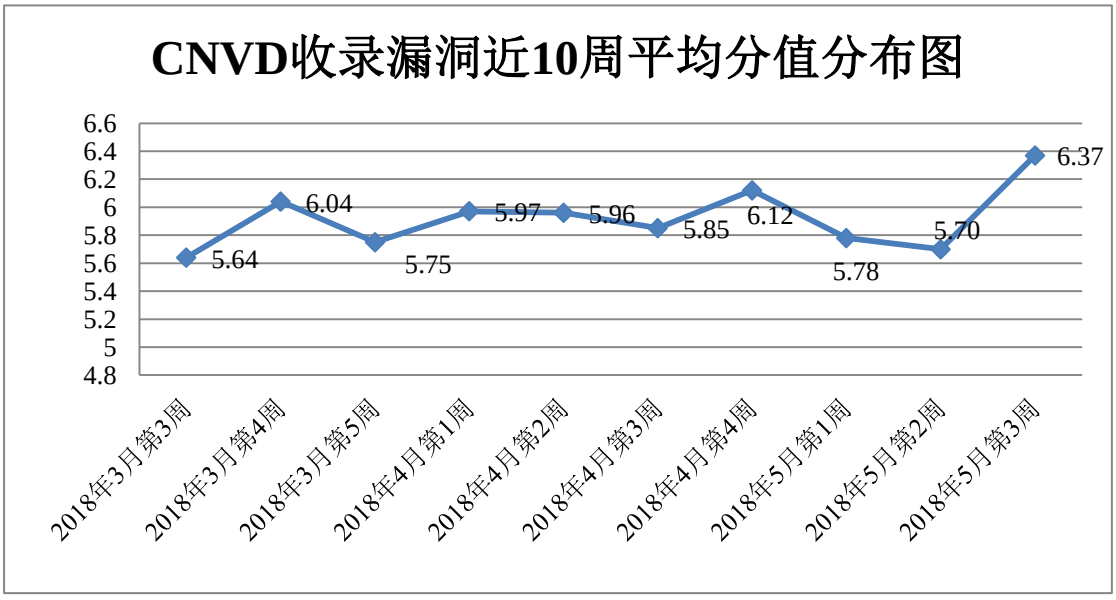

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、北京天融信网络安全技术有限公司、华为技术有限公司、哈尔滨安天科技股份有限公司、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。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、山石网科通信技术有限公司、上海银基信息安全技术股份有限公司、南京联成科技发展股份有限公司、济南三泽信息安全测评有限公司、北京明朝万达科技股份有限公司（安元实验室）、安徽锋刃信息科技有限公司、福建省海峡信息技术有限公司及其他个人白帽子向 CNVD 提交了 540 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 359 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	406	0
北京天融信网络安全技术有限公司	363	3
华为技术有限公司	234	0
360 网神（补天平台）	286	286
哈尔滨安天科技股份有限公司	203	0
北京神州绿盟科技有限公司	147	0
中国电信集团系统集成有限责任公司	144	0
北京数字观星科技有限公司	97	0
新华三技术有限公司	95	0
漏洞盒子	73	73
恒安嘉新(北京)科技股份公司	19	0
厦门服云信息科技有限公司	32	0
北京无声信息技术有限公司	15	0
深圳市腾讯计算机系统有限公司（玄武实验室）	10	10
四川虹微技术有限公司（子午攻防实验室）	12	12
中新网络信息安全股份有限公司	7	7

山石网科通信技术有限公司	6	6
上海银基信息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
济南三泽信息安全测评有限公司	3	3
北京明朝万达科技股份有限公司（安元实验室）	2	2
安徽锋刃信息科技有限公司	2	2
福建省海峡信息技术有限公司	1	1
CNCERT 吉林分中心	6	6
CNCERT 上海分中心	3	3
CNCERT 贵州分中心	2	2
CNCERT 河北分中心	1	1
CNCERT 浙江分中心	1	1
个人	116	116
报送总计	2292	540

本周漏洞按类型和厂商统计

本周，CNVD 收录了 353 个漏洞。其中应用程序漏洞 183 个，WEB 应用漏洞 60 个，操作系统漏洞 54 个，网络设备漏洞 41 个，安全产品漏洞 15 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	183
WEB 应用漏洞	60
操作系统漏洞	54
网络设备漏洞	41
安全产品漏洞	15

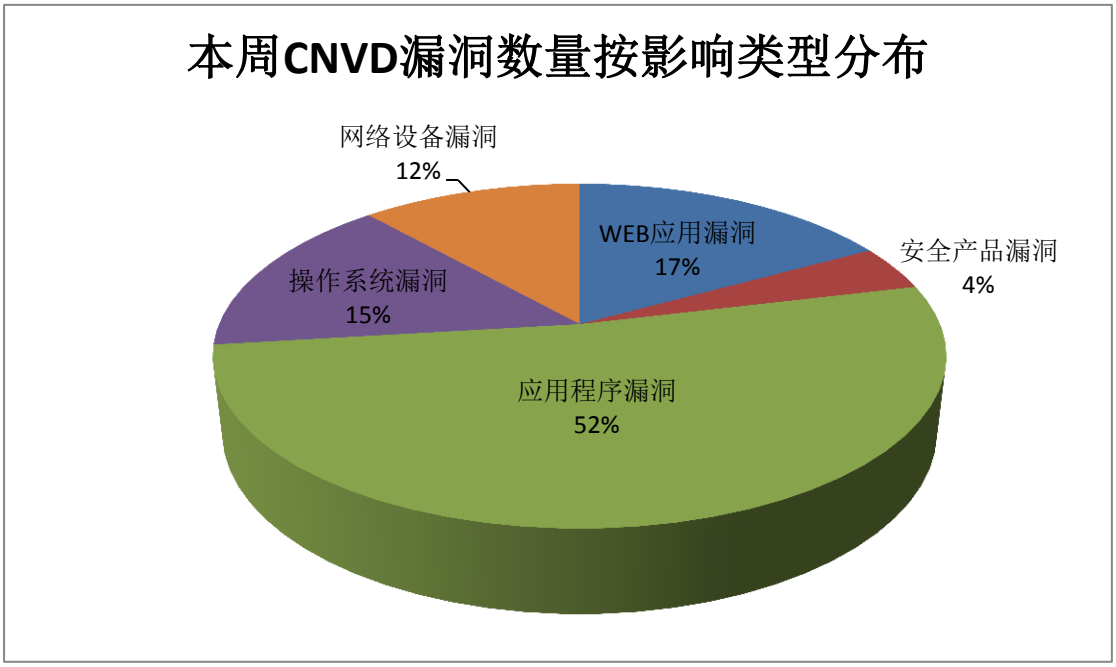

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Apple、Cisco 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	31	9%
2	Apple	18	5%
3	Cisco	17	5%
4	Microsoft	15	4%
5	2345 安全卫士	8	2%
6	F5	8	2%
7	Nagios	8	2%
8	Pivotal Software	7	2%
9	Exiv2	6	2%
10	其他	235	67%

本周行业漏洞收录情况

本周，CNVD 收录了 24 个电信行业漏洞，50 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Moxa EDR-810 拒绝服务漏洞、Buffalo WZR-1750DHP2 任意代码执行漏洞、MyScript SDK for Android 反序列化代码执行漏洞、Siemens SIMATIC

S7-400 拒绝服漏洞、多款 ASUS 产品任意代码执行漏洞”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/

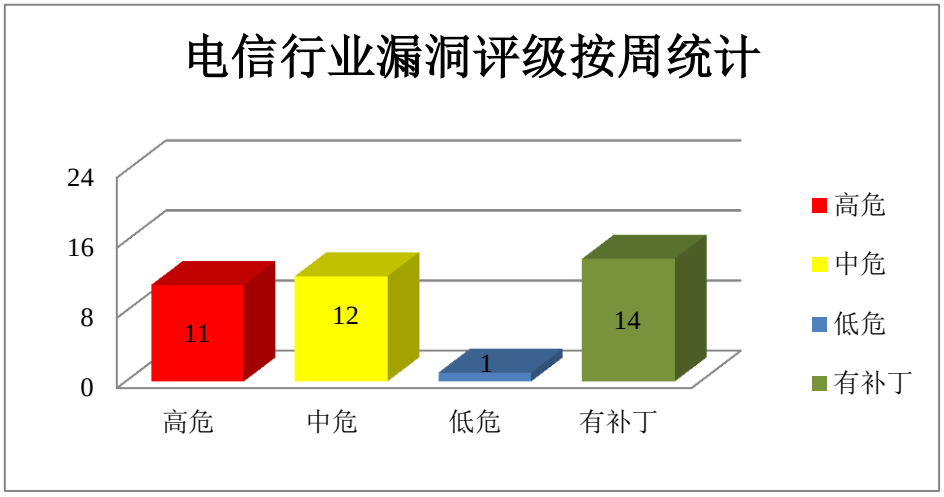

图 3 电信行业漏洞统计

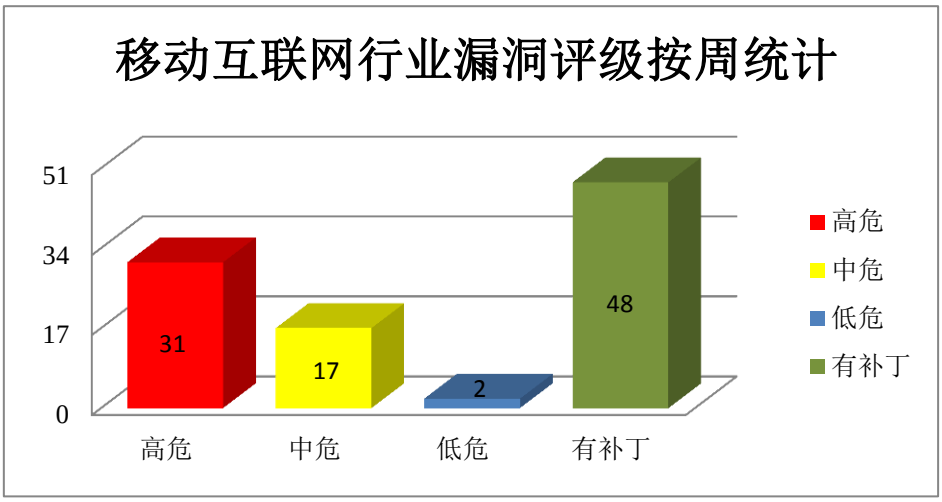

图 4 移动互联网行业漏洞统计

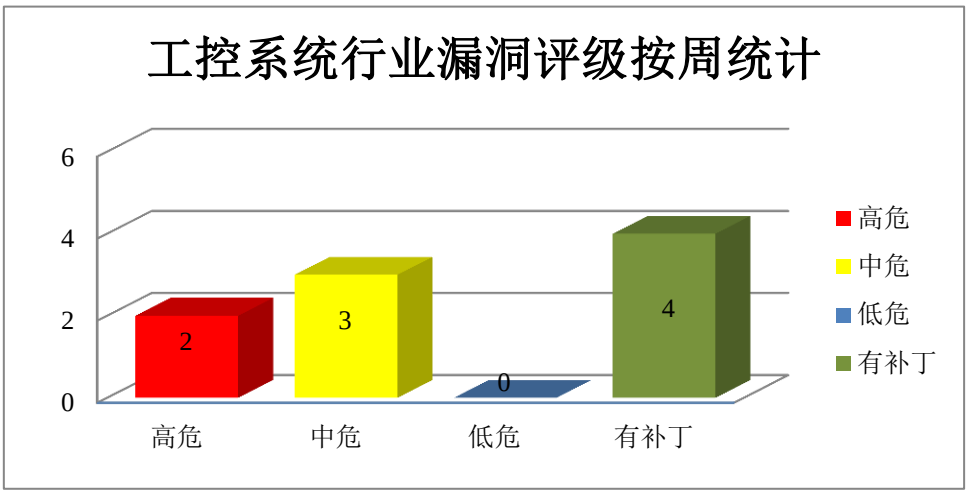

图 5 工控行业漏洞统计

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。本周，上述产品被披露存在权限提升、拒绝服务和缓冲区溢出漏洞，攻击者可利用漏洞提升权限、执行任意代码或造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android mnh 驱动程序提权漏洞、Google Android pci sysfs 权限提升漏洞、Google Android System(system ui)拒绝服务漏洞、Google Android 缓冲区溢出漏洞（CNVD-2018-09703、CNVD-2018-09752、CNVD-2018-09755、CNVD-2018-09778）、Google Android 缓冲区越边界读取漏洞，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-2018-09571

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09572

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09465

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09703

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09752

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09755

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09778

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09705

2、Microsoft 产品安全漏洞

Microsoft Windows 7 和 Microsoft Windows Server 2012 都是美国微软（Microsoft）公司发布的一系列操作系统。Internet Explorer（IE）是其中的一款 Windows 操作系统附带的 Web 浏览器。Microsoft SharePoint Enterprise Server 2016 是一套企业业务协作平台。Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。Microsoft Excel 2010 SP2 是其中一套电子表格处理软件。本周，上述产品被披露存在权限提升和远程代码执行漏洞，攻击者可利用漏洞执行任意代码或提升权限。

CNVD 收录的相关漏洞包括：Microsoft Edge 任意代码执行漏洞（CNVD-2018-09476）、Microsoft Excel 远程代码执行漏洞（CNVD-2018-09644、CNVD-2018-09655）、Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2018-09474）、Microsoft Office 远程代码执行漏洞（CNVD-2018-09645、CNVD-2018-09646）、Microsoft SharePoint 特权提升漏洞、Microsoft Windows VBScript 引擎远程代码执行漏洞。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-2018-09476

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09644

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09655

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09474

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09645

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09646

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09660

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09636

3、Apple 产品安全漏洞

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；Apple iOS 是为移动设备所开发的一套操作系统；tvOS 是一套智能电视操作系统；watchOS 是一套智能手表操作系统。本周，上述产品被披露存在内存破坏和安全绕过漏洞，攻击者可利用该漏洞绕过安全限制或执行任意代码。

CNVD 收录的相关漏洞包括：Apple iOS Web App 安全绕过漏洞、Apple iOS、tv OS 和 watchOS Graphics Driver 内存破坏漏洞、Apple macOS Disk Management 密码截断漏洞、Apple macOS High Sierra Security 代码执行漏洞、Apple macOS High Sierra Touch Bar Support 内存破坏漏洞、多款 Apple 产品 CFNetwork Session 内存破坏漏洞、多款 Apple 产品 CoreAnimation 内存破坏漏洞、多款 Apple 产品 System Preferences 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-2018-09815

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09804

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09803

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09790

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09793

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09791

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09789

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09812

4、Cisco 产品安全漏洞

Cisco Digital Network Architecture Center（DNA Center）是美国思科（Cisco）公司的一套数字网络体系结构解决方案。Cisco Identity Services Engine（ISE）是一款基于身份的环境感知平台。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、泄露敏感信息或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Adaptive Security Appliance Software 和 Firep

ower Threat Defense Software Transport Layer Security 库输入验证漏洞、Cisco ASR 5700 系列路由器输入验证漏洞、Cisco Digital Network Architecture (DNA) Center 安全绕过漏洞 、Cisco Digital Network Architecture (DNA) Center 权限提升漏洞、Cisco Digital Network Architecture (DNA) Center 信息泄露漏洞、Cisco Identity Services Engine 配置错误漏洞、多款 Cisco Industrial Ethernet 交换机跨站请求伪造漏洞、多款 Cisco 产品 Adaptive Security Appliance 和 Firepower Threat Defense Software 拒绝服务漏洞。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-2018-09396

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09782

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09723

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09721

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09722

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09383

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09787

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09673

5、Foscam C1 Indoor HD Camera 固件恢复未签名图像漏洞

Foscam C1 Indoor HD Camera 是中国福斯康姆（Foscam）公司的一款无线高清 IP 摄像机。本周，Foscam 被披露存在恢复未签名图像漏洞，攻击者可通过使用自定义图像恢复固件利用该漏洞完全控制设备。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-2018-09719

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-2018-09401	Vaultize Enterprise File Sharing 文件创建漏洞	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：http://www.vaultize.com/
CNVD-2018-09477	Buffalo WZR-1750DHP2 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，补丁获取链接：http://buffalo.jp/support_s/s20180328.html
CNVD-2018-09541	Red Hat DHCP 客户端命令执行漏洞	高	用户可联系供应商获得补丁信息：https://access.redhat.com/security/vulnerabilities/3442151
CNVD-201	Silex SD-320AN 和 GE Mobil	高	目前厂商已发布升级补丁以修复漏

8-09554	eLink 远程代码执行漏洞		洞，详情请关注厂商主页：https://www.silextechnology.com/
CNVD-2018-09575	runV for Docker util.c 文件权限提升漏洞	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://github.com/hyperhq/runv
CNVD-2018-09587	Pivotal Greenplum Command Center SQL 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://pivotal.io/security/cve-2018-1280
CNVD-2018-09600	Pivotal Spring-integration-zip 任意文件写入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://pivotal.io/security/cve-2018-1261
CNVD-2018-09639	MyScript SDK for Android 反序列化代码执行漏洞	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.myscript.com/sdk/
CNVD-2018-09806	多款 ASUS 产品任意代码执行漏洞	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.asus.com
CNVD-2018-09817	Mautic CSV 注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/mautic/mautic/releases/tag/2.13.0

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、执行任意代码或造成拒绝服务等。此外，Microsoft、Apple、Cisco 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，Foscam 被披露存在恢复未签名图像漏洞，攻击者可通过使用自定义图像恢复固件利用该漏洞完全控制设备。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. 西门子 SIMATIC-S7-400 现严重的 DoS 漏洞

西门子 2018 年 5 月 15 日发布安全公告通知客户，其部分 SIMATIC S7-400 CPU 受严重的拒绝服务（DoS）漏洞影响，该漏洞编号为 CVE-2018-4850，CVSS（V3.0）评分 7.5 分。漏洞原因在于受影响的 CPU 未正确验证 S7 通信数据包，从而允许远程攻击者触发 DoS 条件，可致系统进入并保持 DEFECT 模式，必须手动重启才能恢复。攻击者成功利用该漏洞的前提是能够将特质的 S7 恶意通信数据包发送至 CPU 的通信接口，包括以太网、PROFIBUS 和多点接口（MPI）。值得注意的是，攻击者无需用户交互或获取特权就能利用该漏洞。西门子指出，该漏洞可能会造成 CPU 的核心功能出现拒绝服务状态，从而影响系统的可用性。截至安全公告发布之时，西门子称未发现

公开已知的利用案例。

参考链接：https://www.easyaq.com/news/1873700130.shtml

2. 电子邮件加密工具 PGP 和 S/MIME 被曝严重漏洞

德国明斯特大学的研究人员 2018 年 5 月 13 日发推特警告称，PGP 和 S/MIME 电子邮件加密工具中存在严重的漏洞， 20 多个邮件客户端受到影响。研究人员表示，攻击者可借此发起 EFAIL 攻击，解密发送或接收的加密信息。该漏洞已被电子前沿基金会（EFF）证实。攻击者可利用受害者自己的电子邮件客户端解密先前获取的消息，并将解密后的内容返回给攻击者，而不会提醒受害者。

参考链接：https://www.easyaq.com/news/866620463.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