国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 4 月 30 日-2018 年 5 月 6 日　　2018 年第 18 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 244 个，其中高危漏洞 79 个、中危漏洞 140 个、低危漏洞 25 个。漏洞平均分值为 5.78。本周收录的漏洞中，涉及 0day 漏洞 83 个（占 34%），其中互联网上出现“SIMATIC S 7-400 PLC 存在拒绝服务漏洞、D-Link DIR-815 跨站脚本漏洞（CNVD-2018-08947）”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 534 个，与上周（564 个）环比下降 5%。

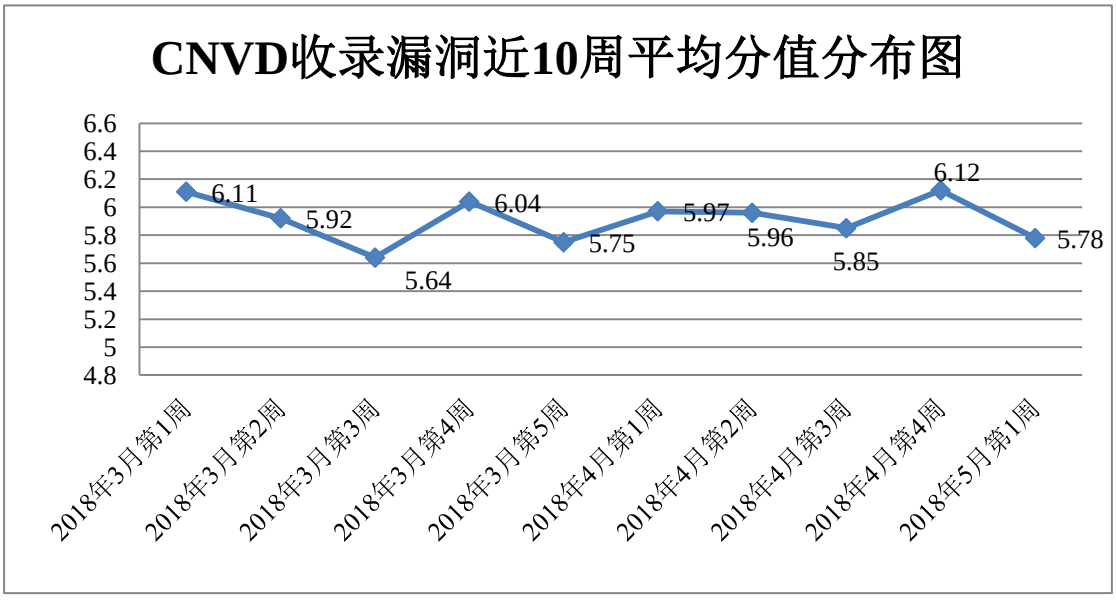

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、北京数字观星科技有限公司、哈尔滨安天科技股份有限公司、杭州安恒信息技术有限公司、北京天融

信网络安全技术有限公司等单位报送公开收集的漏洞数量较多。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、四川虹微技术有限公司（子午攻防实验室）、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 534 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 439 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
漏洞盒子	240	240
360 网神（补天平台）	199	199
北京启明星辰信息安全技术有限公司	149	0
北京数字观星科技有限公司	136	0
哈尔滨安天科技股份有限公司	116	0
杭州安恒信息技术有限公司	81	0
北京天融信网络安全技术有限公司	68	0
新华三技术有限公司	67	0
中国电信集团系统集成有限责任公司	64	0
北京神州绿盟科技有限公司	52	0
华为技术有限公司	45	0
恒安嘉新(北京)科技股份公司	25	0
阿里云计算有限公司	20	0
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	8	0
中新网络信息安全股份有限公司	5	5
山石网科通信技术有限公司	5	5

四川虹微技术有限公司（子午攻防实验室）	3	3
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 新疆分中心	3	3
CNCERT 河北分中心	2	2
个人	74	74
报送总计	1376	534

本周漏洞按类型和厂商统计

本周，CNVD 收录了 244 个漏洞。其中应用程序漏洞 116 个，WEB 应用漏洞 68 个，操作系统漏洞 35 个，网络设备漏洞 24 个，安全产品漏洞 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	116
WEB 应用漏洞	68
操作系统漏洞	35
网络设备漏洞	24
安全产品漏洞	1

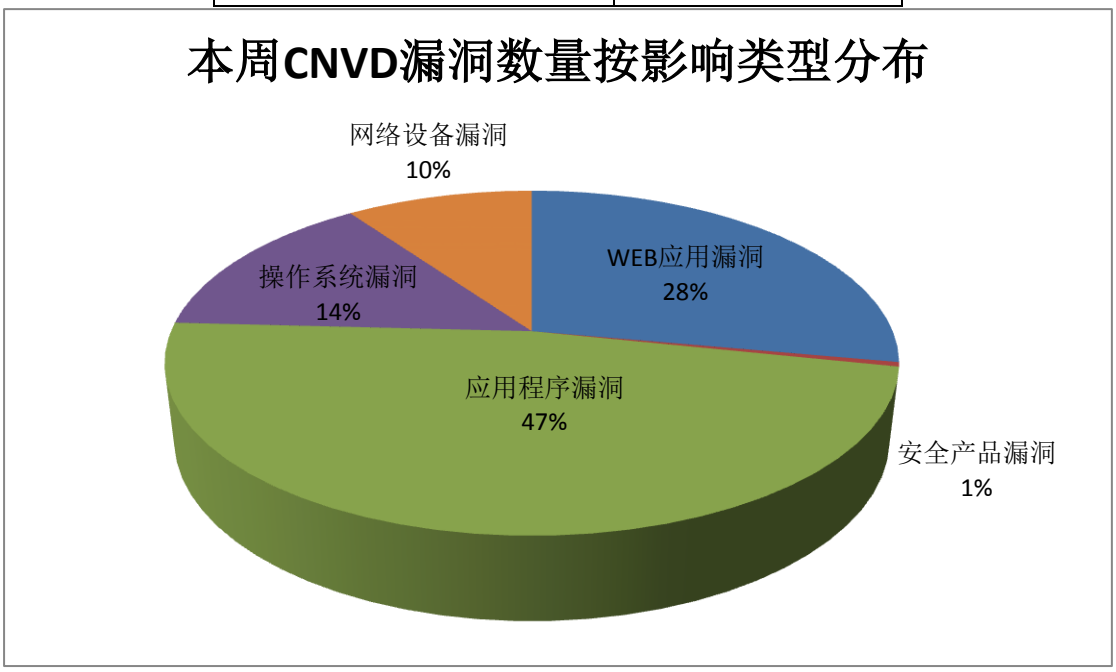

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Google、Cms made simple 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	25	10%
2	Google	24	10%
3	Cms made simple	15	6%
4	IBM	14	6%
5	SAP	8	3%
6	Cisco	7	3%
7	Computerinsel	7	3%
8	Cybozu	5	2%
9	iScripts	5	2%
10	其他	134	55%

本周行业漏洞收录情况

本周，CNVD 收录了 13 个电信行业漏洞，16 个移动互联网行业漏洞，13 个工控行业漏洞（如下图所示）。其中，“CyberArk Password Vault Web Access 远程代码执行漏洞、多款 Apple 产品 WebKit 用户界面伪造漏洞、Google Android 缓冲区溢出漏洞（CNVD-2018-08829）、和利时 LE5109L PLC 存在拒绝服务漏洞、MAC1100 PLC 存在远程控制漏洞”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/

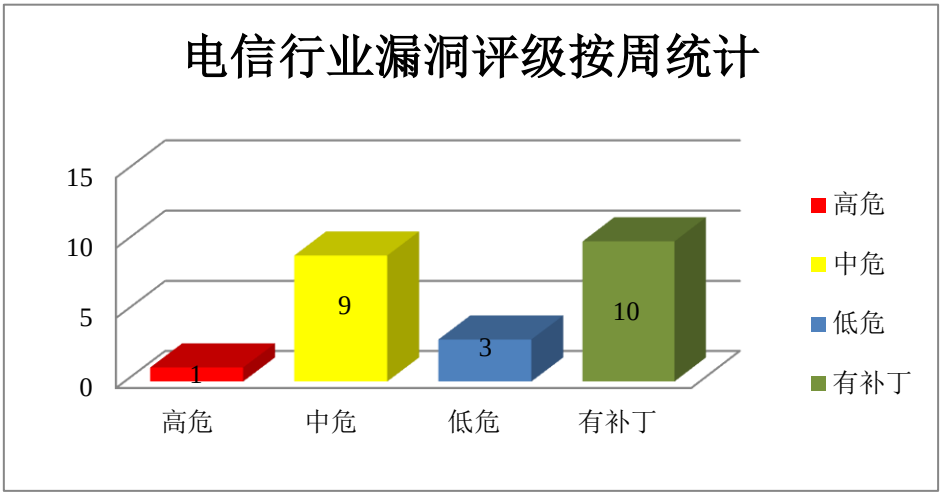

图 3 电信行业漏洞统计

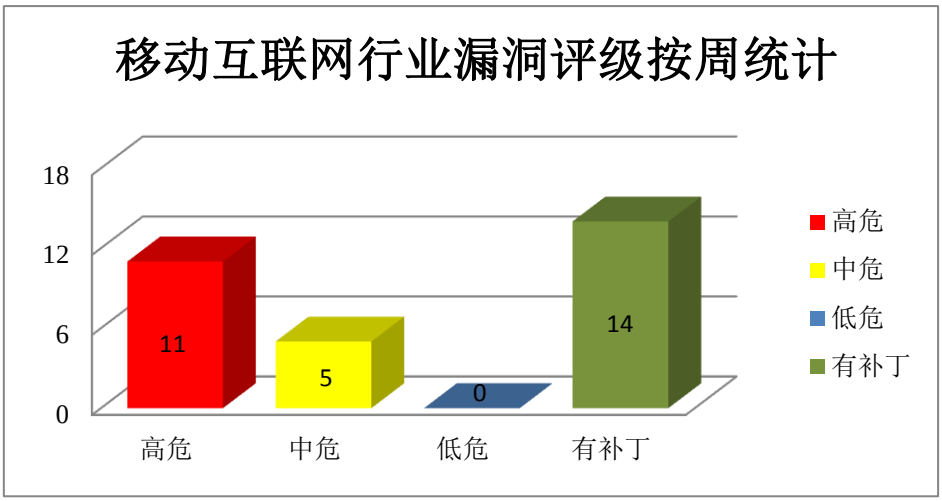

图 4 移动互联网行业漏洞统计

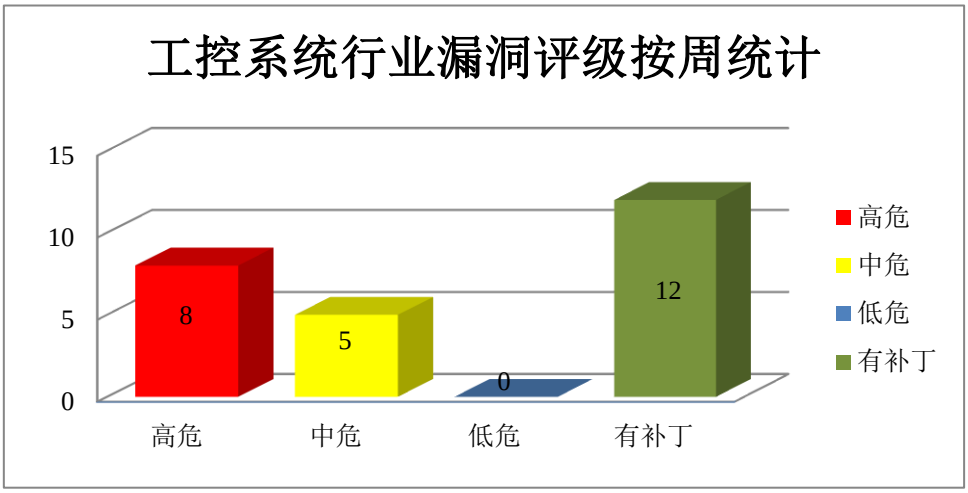

图 5 工控行业漏洞统计

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，该产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞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 缓冲区溢出漏洞（CNVD-2018-08825、CNVD-2018-08826、CNVD-2018-08827、CNVD-2018-08828、CNVD-2018-08829、CNVD-2018-08830、CNVD-2018-08831、CNVD-2018-08832）。该漏洞的综合评级为“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-2018-08825

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08826

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08827

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08828

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08829

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08830

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08831

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08832

2、Microsoft 产品安全漏洞

Microsoft Excel 是微软公司的办公软件 Microsoft office 的组件之一。SharePoint 是微软制作的一款用于 Windows Server 2003 的免费附加（增值）软件。Microsoft Windows 10 是一套供个人电脑使用的操作系统，indows Server 2016 是一套服务器操作系统。本周，上述产品被披露存在远程代码执行和权限提升漏洞，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 ChakraCore 和 Edge 远程代码执行漏洞（CNVD-2018-08796、CNVD-2018-08797）、Microsoft Excel 和 Office 远程代码执行漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2018-08761、CNVD-2018-08937）、Microsoft SharePoint 权限提升漏洞（CNVD-2018-08793、CNVD-2018-08794、CNVD-2018-08795）。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-2018-08796

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08797

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08803

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08761

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08937

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08793

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08794

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08795

3、IBM 产品安全漏洞

IBM Security QRadar SIEM 是美国 IBM 公司的一套可对分散在整个网络中的数千个设备和应用中的日志源事件数据进行整合的解决方案。BM Campaign 是一套用于帮助营销人员设计、执行、衡量和优化营销广告的管理解决方案。IBM BigFix platform 是一套动态的集成了消息内容驱动和管理系统的多技术平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息、执行任意代码或进行跨站脚本攻击等。

CNVD 收录的相关漏洞包括：IBM QRadar SIEM SQL 注入漏洞（CNVD-2018-08915）、IBM QRadar SIEM 远程代码执行漏洞、IBM QRadar SIEM 跨站脚本漏洞（CNVD-2018-08913）、IBM QRadar SIEM 目录遍历漏洞、IBM BigFix Platform 信息泄露漏洞（CNVD-2018-08938）、IBM Campaign 信息泄露漏洞、IBM Content Manager 跨站脚本漏洞、IBM API Connect 跨站脚本漏洞（CNVD-2018-08943）。其中，“IBM QRadar SIEM SQL 注入漏洞（CNVD-2018-08915）、IBM QRadar SIEM 远程代码执行漏洞”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-2018-08915

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08916

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08913

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08914

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08938

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08928

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08919

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08943

4、SAP 产品安全漏洞

SAP Disclosure Management 是德国思爱普（SAP）公司的一套自动化财务披露管理系统。SAP Crystal Reports Server OEM Edition（CRSE）是一套报表解决方案。SAP Cloud Platform 是一套开放式平台即服务（PaaS）式云平台。SAP Solution Manager 是一套集系统监控、SAP 支持桌面、自助服务、ASAP 实施等多个功能为一体的系统管理平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏上传任意文件、提升权限或进行跨站脚本攻击等。

CNVD 收录的相关漏洞包括：SAP Disclosure Management 文件上传漏洞、SAP Disclosure Management 权限提升漏洞、SAP Disclosure Management 权限提升漏洞（CNVD-2018-08888）、SAP Disclosure Management 未授权访问漏洞、SAP Solution Manager Incident Management Work Center 跨站脚本漏洞、SAP Business Objects 会话固定漏洞、

SAP Cloud Platform 会话固定漏洞、SAP Crystal Reports Server OEM Edition 本地权限提升漏洞。其中“SAP Disclosure Management 文件上传漏洞、SAP Disclosure Management 权限提升漏洞、SAP Disclosure Management 权限提升漏洞（CNVD-2018-08888）”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-2018-08878

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08887

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08888

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08883

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08945

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08897

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08886

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08882

5、SIMATIC S7-400 PLC 存在拒绝服务漏洞

SIMATIC S7-400 PLC 是是用于中、高档性能范围的可编程序控制器。本周，SIMATIC 被披露存在拒绝服务漏洞，攻击者可利用漏洞处理特定的标签变量写操作（Write Var）导致系统宕机。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-2018-08790

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-2018-08712	Navarino Infinity 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://navarino.gr/archives/6989
CNVD-2018-08806	Kentico 信息泄露漏洞	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.kentico.com/
CNVD-2018-08835	Apple MacOS 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://support.apple.com/en-us/HT208742
CNVD-2018-08873	多款 Apple 产品 WebKit 用户界面伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.apple.com/zh-cn/HT208324
CNVD-201	Apple Safari WebKit Web Ins	高	目前厂商已发布升级补丁以修复漏

8-08874	pector 任意代码执行漏洞		洞，补丁获取链接：https://support.apple.com/zh-cn/HT208324
CNVD-2018-08903	Atlassian JIRA Server 安全绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jira.atlassian.com/browse/JRASERVER-67107
CNVD-2018-08904	Open Web Analytics 堆缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.openwebanalytics.com/?p=388
CNVD-2018-08915	IBM QRadar SIEM SQL 注入漏洞（CNVD-2018-08915）	高	厂商已发布漏洞修复程序，请及时关注更新：http://www-01.ibm.com/support/docview.wss?uid=swg22015802
CNVD-2018-08916	IBM QRadar SIEM 远程代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://www-01.ibm.com/support/docview.wss?uid=swg22015799
CNVD-2018-08950	Simple DirectMedia Layer SDL2_image 代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.libsdl.org/projects/SDL_image/

小结：本周， Google 被披露存在缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码或造成拒绝服务。此外，Microsoft、IBM、SAP 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、提升权限或进行跨站脚本攻击等。另外，SIMATIC 被披露存在拒绝服务漏洞，攻击者可利用漏洞处理特定的标签变量写操作（Write Var）导致系统宕机。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. 英特尔 CPU 再曝 8 个“幽灵+”漏洞，影响亚马逊等云服务提供商

Google Project Zero 安全研究团队在英特尔 CPU 中又发现 8 个新的“幽灵式”硬件漏洞，被称为“新一代幽灵”——Spectre-NG（4 个高危，4 个中危漏洞），其中一个漏洞非常严重，允许攻击者在虚拟机中执行恶意代码，进而攻击读取宿主机的数据。此外，攻击者可以攻击在同一台服务器上运行的其它客户的虚拟机。黑客很容易盯上云系统上用于数据安全传输的密码和密钥。无论英特尔的软件防护扩展（SGX）功能是否启用，Spectre-NG 都能被利用。oogle Project Zero 预计会在在下周发布技术细节。英特尔正在准备补丁。此外，英特尔已承诺会重新构建处理器，防止出现“幽灵”和“熔断”漏洞。

参考链接：https://www.easyaq.com/news/283148343.shtml

2. 施耐德电气软件被曝远程代码执行漏洞

网络安全公司 Tenable 2018 年 5 月 2 日披露，两款施耐德电气软件存在远程代码执行漏洞，可能会被黑客利用干扰或破坏发电厂、供水系统和太阳能设施等基础设施。此次的远程代码执行漏洞和两个工具中的一个功能有关，该功能允许 HMI 客户端读取并写入标签并监控警报和事件消息。目前尚不清楚有多少个系统为软件打了补丁。Tenable 公司的研究人员表示，他们目前尚未发现网络攻击利用这个漏洞，但也没有办法确切地知道，除非有受害者站出来披露。

参考链接：https://www.easyaq.com/news/1670162341.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