国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 6 月 11 日-2018 年 6 月 17 日 **2018 年第 24 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 302 个，其中高危漏洞 109 个、中危漏洞 179 个、低危漏洞 14 个。漏洞平均分值为 6.28。本周收录的漏洞中，涉及 0day 漏洞 74 个（占 25%），其中互联网上出现“MACCMS 10 跨站请求伪造漏洞、WordPress Pie Register 插件 SQL 注入漏洞”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 477 个，与上周（630 个）环比下降 24 %。

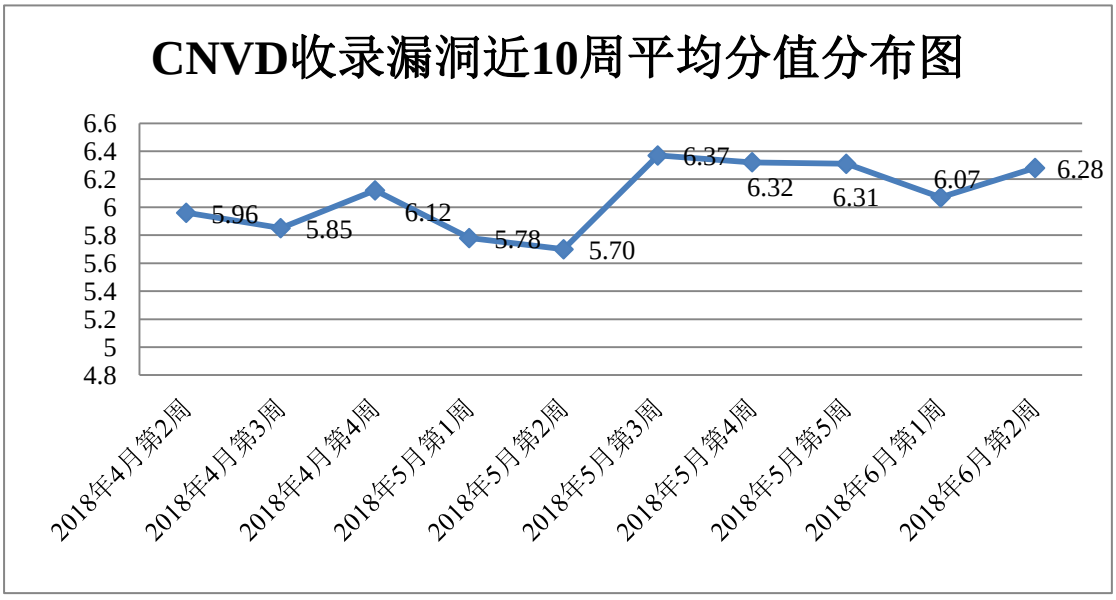

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、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、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。中新网络信息安全股份有限公司、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）、任子行网络技术股份有限公司、河南信安世纪科技有限公司、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、北京智游网安科技有限公司、海南上德科技有限公司、福建六壬网安股份有限公司及其他个人白帽子向 CNVD 提交了 477 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 317 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	373	0
杭州安恒信息技术有限公司	339	0
北京天融信网络安全技术有限公司	305	0
哈尔滨安天科技股份有限公司	250	0
漏洞盒子	166	166
360 网神（补天平台）	151	151
华为技术有限公司	130	0
北京数字观星科技有限公司	99	0
新华三技术有限公司	97	0
恒安嘉新(北京)科技股份公司	69	0
北京启明星辰信息安全技术有限公司	52	0
北京神州绿盟科技有限公司	36	0
中国电信集团系统集成有限责任公司	36	3
北京无声信息技术有限公司	17	0
厦门服云信息科技有限公司	14	0

阿里云计算有限公司	5	0
北京知道创宇信息技术有限公司	2	1
中新网络信息安全股份有限公司	13	13
南京联成科技发展股份有限公司	13	13
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	2	2
河南信安世纪科技有限公司	2	2
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
北京智游网安科技有限公司	1	1
海南上德科技有限公司	1	1
福建六壬网安股份有限公司	1	1
CNCERT 新疆分中心	10	10
CNCERT 山西分中心	5	5
CNCERT 湖南分中心	3	3
CNCERT 海南分中心	3	3
CNCERT 辽宁分中心	2	2
个人	92	92
报送总计	2297	477

本周漏洞按类型和厂商统计

本周，CNVD 收录了 302 个漏洞。其中应用程序漏洞 184 个，操作系统漏洞 40 个，WEB 应用漏洞 37 个，网络设备漏洞 29 个，安全产品漏洞 11 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	184
操作系统漏洞	40
WEB 应用漏洞	37
网络设备漏洞	29
安全产品漏洞	11
数据库漏洞	1

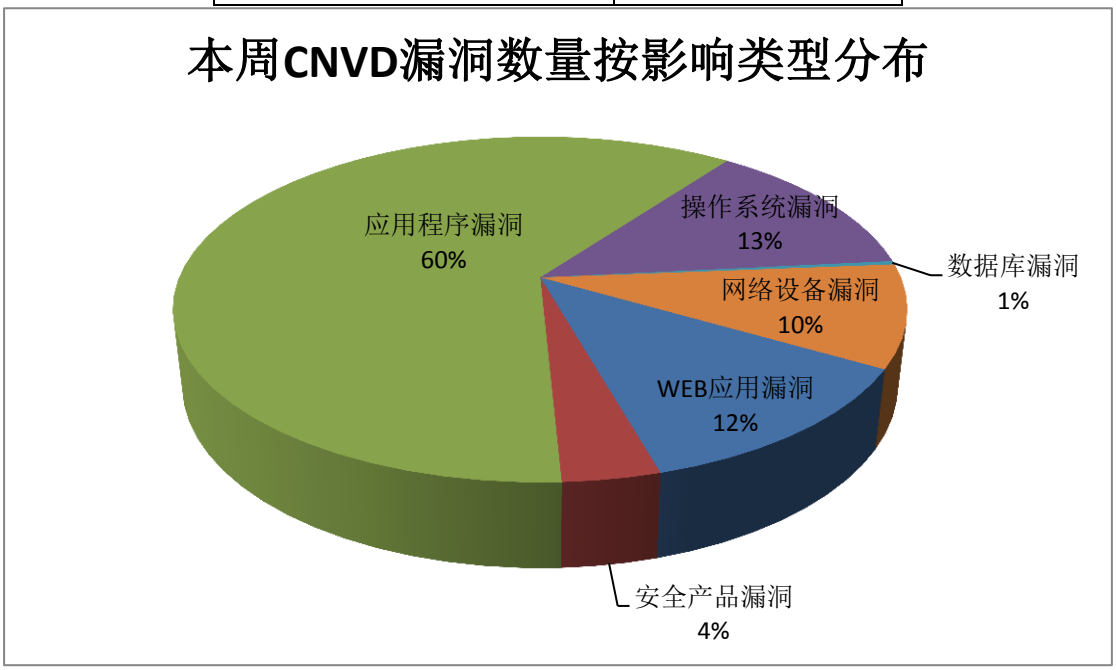

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Cisco、Google、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	Cisco	38	13%
2	Google	25	8%
3	Microsoft	16	5%
4	SIEMENS	11	4%
5	Apple	11	4%
6	WordPress	9	3%
7	Schneider Electric	8	2%
8	Bayerische Motoren Werke AG	7	2%
9	Linux	6	2%

10	其他	171	57%

本周行业漏洞收录情况

本周，CNVD 收录了 15 个电信行业漏洞，26 个移动互联网行业漏洞，23 个工控行业漏洞（如下图所示）。其中，“SIEMENS SCALANCE M875 命令注入漏洞、Synology Router Manager 命令注入漏洞、Cisco AppDynamics App iQ Platform SQL 注入漏洞、Google Android 权限提升漏洞（CNVD-2018-11357）、SIEMENS SCALANCE M875 跨站请求伪造漏洞”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/

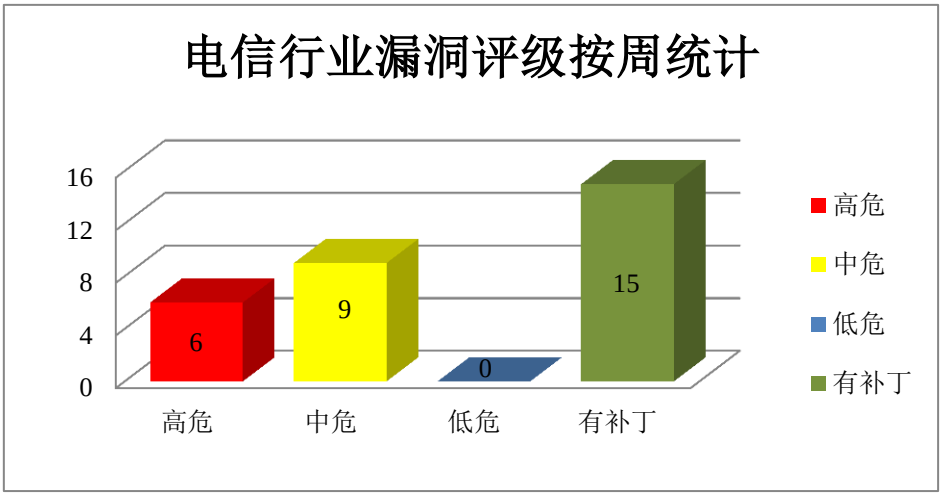

图 3 电信行业漏洞统计

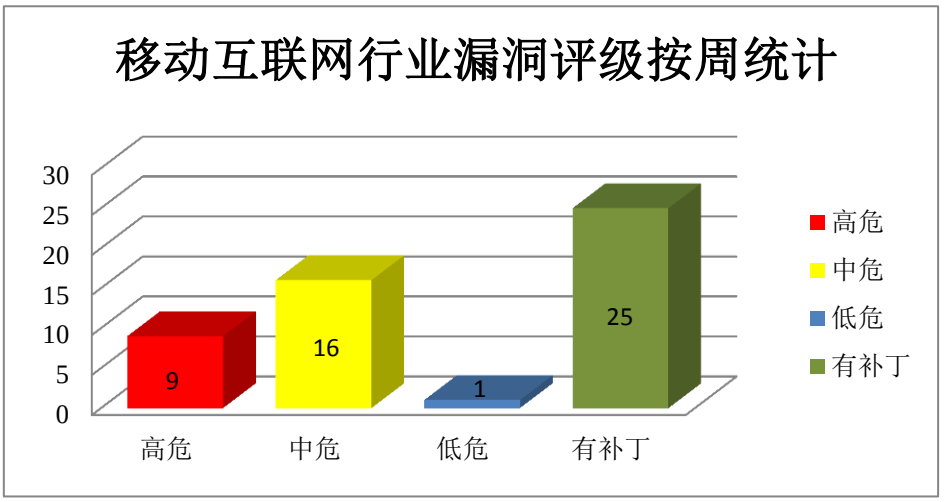

图 4 移动互联网行业漏洞统计

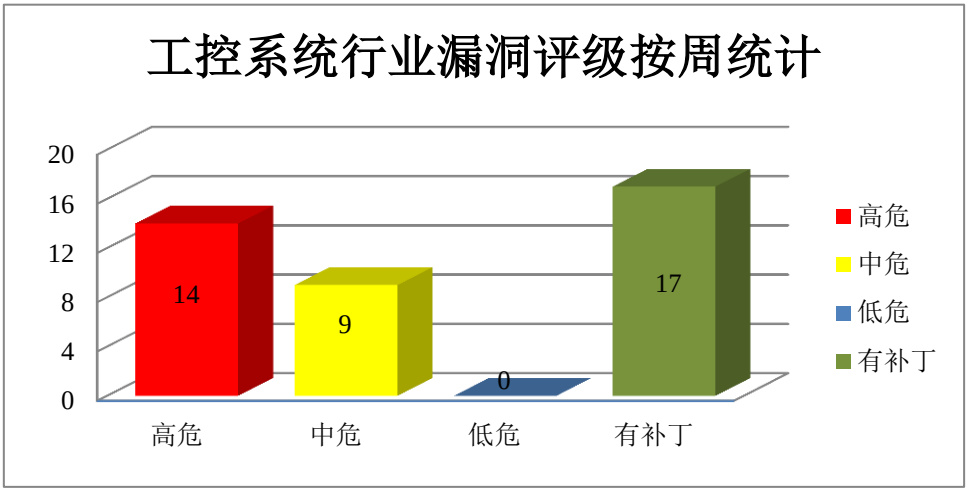

图 5 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco Prime Collaboration Provisioning（PCP）是一套基于 Web 的下一代通信服务软件。Cisco Firepower Threat Defense 是一套运行在防火墙中的软件。detection engine 是其中的一个检测引擎。Cisco Prime Collaboration Provisioning（PCP）是一套基于 Web 的下一代通信服务软件。Cisco AppDynamics App iQ Platform 是一款实时应用程序和业务性能监控解决方案。Cisco Wide Area Application Services（WAAS）Software 是一套广域网链路加速软件。Disk Check Tool（disk-check.sh）是其中的一个磁盘检查工具。Cisco IOS XE Software 是一套为其网络设备开发的操作系统。Cisco IP Phone 6800、7800 和 8800 Series Phones 都是美国思科（Cisco）公司的不同系列的 IP 电话产品。Multiplatform Firmware 是其中的一套支持多平台的防火墙软件。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数据库敏感信息，绕过安全功能限制，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：Cisco Prime Collaboration Provisioning SQL 注入漏洞（CNVD-2018-11254）、Cisco Firepower Threat Defense software 远程安全绕过漏洞、Cisco IP Phone 8800 Series 和 IP Phone 7800 Series 拒绝服务漏洞、Cisco Web Security Appliance AsyncOS 安全绕过漏洞、Cisco AppDynamics App iQ Platform SQL 注入漏洞、Cisco Wide Area Application Services（WAAS）软件权限提升漏洞、Cisco IOS XE Software 缓冲区溢出漏洞、Cisco IP Phone 6800、7800 和 8800 Series Phones 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-2018-11254

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11284

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11288

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11300

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11298

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11318

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11323

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11347

2、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司开发的一款 Web 浏览器。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多个漏洞，攻击者可利用漏洞执行未授权的操作，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 V8 类型混淆漏洞（CNVD-2018-11352）、Google Chrome PDFium 堆缓冲区溢出漏洞（CNVD-2018-11353）、Google Chrome 权限提升漏洞（CNVD-2018-11354）、Google Android 权限提升漏洞（CNVD-2018-11356、CNVD-2018-11480）、Google Chrome Blink UI 欺骗漏洞（CNVD-2018-11482）、Google Chrome 越界内存访问漏洞（CNVD-2018-11486）、Google Chrome Skia 堆缓冲区溢出漏洞（CNVD-2018-11495）。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-2018-11352

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11353

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11354

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11356

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11480

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11482

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11486

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11495

3、Microsoft 产品安全漏洞

Microsoft Windows 10、Windows Server 2016、Windows 7 SP1、Windows Server Version 1803、Windows 7 等都是一系列操作系统。本周，上述产品被披露存在权限提升和远程代码执行漏洞，攻击者可利用漏洞提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Desktop Bridge 权限提升漏洞（CNVD-2018-11545）、Microsoft Windows Kernel 权限提升漏洞（CNVD-2018-11546）、Microsoft Windows Win32k 组件权限提升漏洞、Microsoft Windows Kernel 'Win32k.sys'

本地权限提升漏洞、Microsoft Windows Desktop Bridge 权限提升漏洞、Microsoft Windows 远程代码执行漏洞（CNVD-2018-11554）、Microsoft Windows HIDParser 权限提升漏洞、Microsoft Windows 远程代码执行漏洞（CNVD-2018-11572）。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-2018-11545
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11546
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11547
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11551
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11550
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11554
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11571
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11572

4、Apple 产品安全漏洞

Apple Safari Technology Preview 是一款浏览器。WebKit 是 KDE 社区开发的一套开源 Web 浏览器引擎，目前被 Apple Safari 及 Google Chrome 等浏览器使用。Apple iOS 是一套操作系统。Apple macOS High Sierra 是一套专为 Mac 计算机所开发的专用操作系统。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，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：Apple Safari Technology Preview WebKit 拒绝服务漏洞（CNVD-2018-11311）、Apple iOS Messages 拒绝服务漏洞（CNVD-2018-11369）、Apple macOS High Sierra Accessibility Framework 信息泄露漏洞、Apple macOS High Sierra ATS 类型混淆漏洞、Apple macOS High Sierra Firmware 设备配置漏洞、Apple macOS High Sierra Bluetooth 信息泄露漏洞、多款 Apple 产品 FontParser 内存破坏漏洞、Apple macOS High Sierra Hypervisor 内存破坏漏洞。其中，“Apple macOS High Sierra ATS 类型混淆漏洞、多款 Apple 产品 FontParser 内存破坏漏洞、Apple macOS High Sierra Hypervisor 内存破坏漏洞” 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-2018-11311
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11369
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11575
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11577
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11578
http://www.cnvd.org.cn/flaw/show/CNVD-2018-11582

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11579

http://www.cnvd.org.cn/flaw/show/CNVD-2018-11583

5、Advantech WebAccess 'nvA1Media.ocx'堆栈缓冲区溢出漏洞

Advantech WebAccess 是研华（Advantech）公司的一套基于浏览器架构的 HMI/SCADA 软件。该软件支持动态图形显示和实时数据控制，并提供远程控制和管理自动化设备的功能。本周，Advantech WebAccess 被披露存在堆栈缓冲区溢出漏洞，攻击者可利用漏洞在受影响设备环境中执行任意代码，失败的攻击会造成拒绝服务。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-2018-11442

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-2018-11563	WordPress WP Google Map 插件存在多个 SQL 注入漏洞	高	用户可联系供应商获得补丁信息：https://wordpress.org/plugins/wp-google-map-plugin/
CNVD-2018-11506	多款 Huawei 产品 Intelligent Baseboard Management Controller 权限提升漏洞	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.huawei.com/cn/psirt/security-advisories/huawei-sa-20180530-03-server-cn
CNVD-2018-11469	Trend Micro OfficeScan 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://success.trendmicro.com/solution/1119961
CNVD-2018-11435	Adobe Flash 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://helpx.adobe.com/security/products/flash-player/apsb18-19.html
CNVD-2018-11429	IBM Robotic Process Automation with Automation Anywhere 任意命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www-01.ibm.com/support/docview.wss?uid=swg22016197
CNVD-2018-11403	Novell SUSE Studio Onsite 和 SUSE Studio Onsite Appliance 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://www.suse.com/security/cve/CVE-2011-0467/
CNVD-2018-11393	Schneider Electric U.motion Builder 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：https://www.schneider-electric.com/en/d

			ownload/document/Umotion_Server_update/
CNVD-2018-11370	Synology DiskStation Manager 命令注入漏洞（CNVD-2018-11370）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.synology.cn/en-global/support/security/Synology_SA_18_24
CNVD-2018-11235	Appnitro MachForm SQL 注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.machform.com/blog-machform-423-security-release/
CNVD-2018-11557	Redaxo CMS Mediapool 插件文件上传漏洞	高	用户可联系供应商获得补丁信息：https://redaxo.org

小结：本周，本周，Cisco 被披露存在多个漏洞，攻击者可利用漏洞获取数据库敏感信息，绕过安全功能限制，提升权限，执行任意代码或发起拒绝服务攻击。此外，Google、Microsoft、Apple 等多款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，执行未授权的操作，提升权限，执行任意代码或发起拒绝服务攻击。另外，Advantech WebAccess 被披露存在堆栈缓冲区溢出漏洞，攻击者可利用漏洞在受影响设备环境中执行任意代码，失败的攻击会造成拒绝服务。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. 英特尔公布 Spectre 漏洞新变体 Lazy State

近日，英特尔公开披露了 Spectre 漏洞的新变体 Lazy State，将会影响其旗下的多款处理器产品。该漏洞被称为 Lazy State，并被识别为 CVE-2018-3665。该漏洞可能会使攻击者获取有关应用活动的信息，包括加密内容。Red Hat 硬件架构师 Jon Masters 称：CVE-2018-3665 是一个推测执行漏洞，影响了一些常用的现代微处理器，Red Hat 正在与我们的行业合作伙伴就优化的缓解补丁进行合作，这些补丁将通过我们正常的软件发布机制提供。据悉，该漏洞不会影响 AMD 处理器。

参考链接：https://www.zdnet.com/article/another-day-another-intel-cpu-security-hole-lazy-state/

2. ABB 门禁通信系统曝严重漏洞

ABB IP 网关（同时也以 Busch-Jaeger 品牌销售），它是 ABB 门禁通信解决方案的一个组件。此类解决方案包括音频和视频对讲机、指纹读取器等。安全研究人员披露，瑞士工业技术公司 ABB 的门禁通信系统中存在多个严重漏洞。其中一个漏洞为远程代码注入漏洞，允许访问本地网络的攻击者控制目标设备。该漏洞影响本地配置 Web 服务器，攻击者可向系统发送特制的信息利用该漏洞。

参考链接：https://www.easyaq.com/news/2071564544.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