国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 7 月 30 日-2018 年 8 月 5 日 **2018 年第 31 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 273 个，其中高危漏洞 66 个、中危漏洞 203 个、低危漏洞 4 个。漏洞平均分值为 6.08。本周收录的漏洞中，涉及 0day 漏洞 91 个（占 33%），其中互联网上出现“WordPress 插件 Responsive Thumbnail Slider 任意文件上传漏洞、ShopNx 任意文件上传漏洞”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 534 个，与上周（807 个）环比下降 33%。

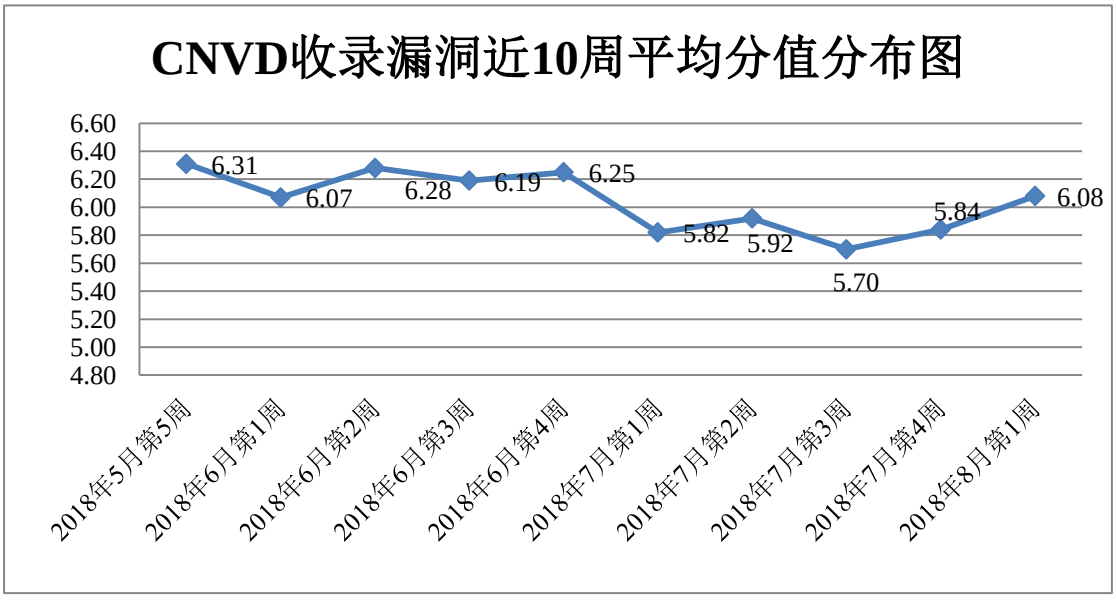

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、哈尔滨安天科技股份有限公司、华为技术有限公司、北京神州绿盟科技有限公司、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、中新网络信息安全股份有限公司、北京国舜科技股份有限公司、南京联成科技发展股份有限公司、上海银基信息安全技术股份有限公司、上海观安信息技术股份有限公司、安徽锋刃信息科技有限公司、北京禹宏信安科技有限公司、河南信安世纪科技有限公司、上海零盾网络科技有限公司、河北盾安科技有限公司、河北网信智安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 237 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	370	16
漏洞盒子	220	220
哈尔滨安天科技股份有限公司	205	0
华为技术有限公司	135	0
北京神州绿盟科技有限公司	99	2
新华三技术有限公司	92	0
北京数字观星科技有限公司	83	0
中国电信集团系统集成有限责任公司	56	0
恒安嘉新(北京)科技股份公司	40	0
深圳市深信服电子科技有限公司	21	0
360 网神（补天平台）	17	17
北京知道创宇信息技术有限公司	17	17
沈阳东软系统集成工程有限公司	9	9
厦门服云信息科技有限公司	4	0
北京无声信息技术有限公司	2	0
北京启明星辰信息安全技术有限公司	1	1

山东云天安全技术有限公司	92	92
中新网络信息安全股份有限公司	11	11
北京国舜科技股份有限公司	7	7
南京联成科技发展股份有限公司	4	4
上海银基信息安全技术股份有限公司	3	3
上海观安信息技术股份有限公司	2	2
安徽锋刃信息科技有限公司	2	2
北京禹宏信安科技有限公司	1	1
河南信安世纪科技有限公司	1	1
上海零盾网络科技有限公司	1	1
河北盾安科技有限公司	1	1
河北网信智安信息技术有限公司	1	1
CNCERT 吉林分中心	9	9
CNCERT 四川分中心	6	6
CNCERT 海南分中心	3	3
CNCERT 新疆分中心	3	3
CNCERT 山西分中心	1	1
CNCERT 贵州分中心	1	1
个人	103	103
报送总计	1623	534

本周漏洞按类型和厂商统计

本周，CNVD 收录了 273 个漏洞。应用程序漏洞 179 个，网络设备漏洞 59 个，WEB 应用漏洞 26 个，操作系统漏洞 6 个，安全产品漏洞 2 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	179
网络设备漏洞	59
WEB 应用漏洞	26
操作系统漏洞	6
安全产品漏洞	2
数据库漏洞	1

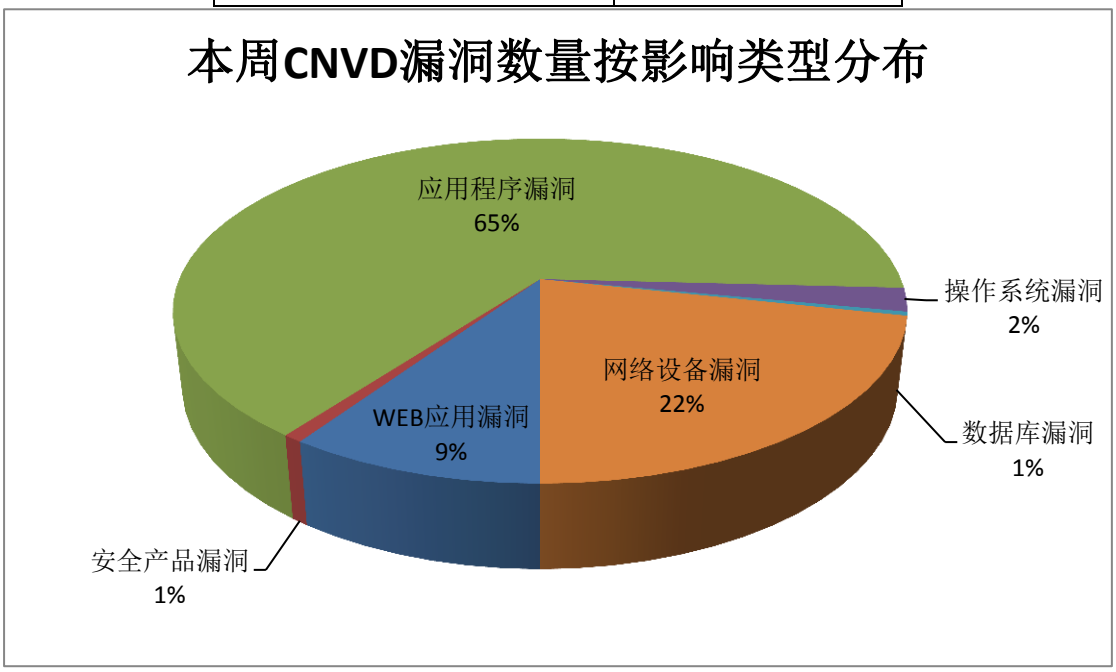

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Foxit、Cisco、Samsung 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	37	14%
2	Cisco	23	9%
3	Samsung	14	5%
4	Adobe	12	4%
5	SAP	7	3%
6	FastStone	6	2%
7	WordPress	5	2%
8	Google	4	1%
9	Oracle	4	1%

10	其他	161	59%

本周行业漏洞收录情况

本周，CNVD 收录了 15 个电信行业漏洞，8 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“Davolink DVW-3200N 路由器弱密码漏洞、Cisco Nexus 3000 和 9000 Series Switches NX-OS 拒绝服务漏洞、Android Qualcomm WLAN 缓冲区溢出漏洞、WECON（维控）LeviStudioU 栈堆缓冲区溢出漏洞、多款 Cisco 产品 NX-OS Software CLI 解析器输入验证漏洞”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/

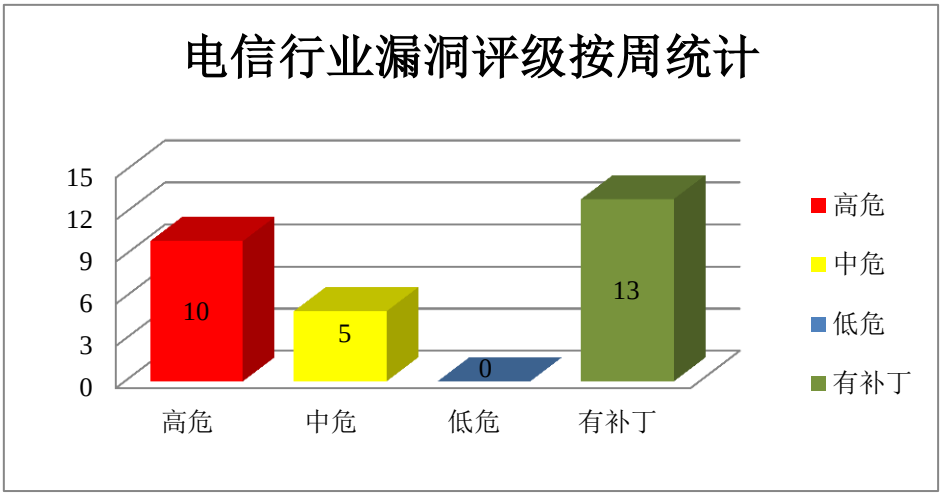

图 3 电信行业漏洞统计

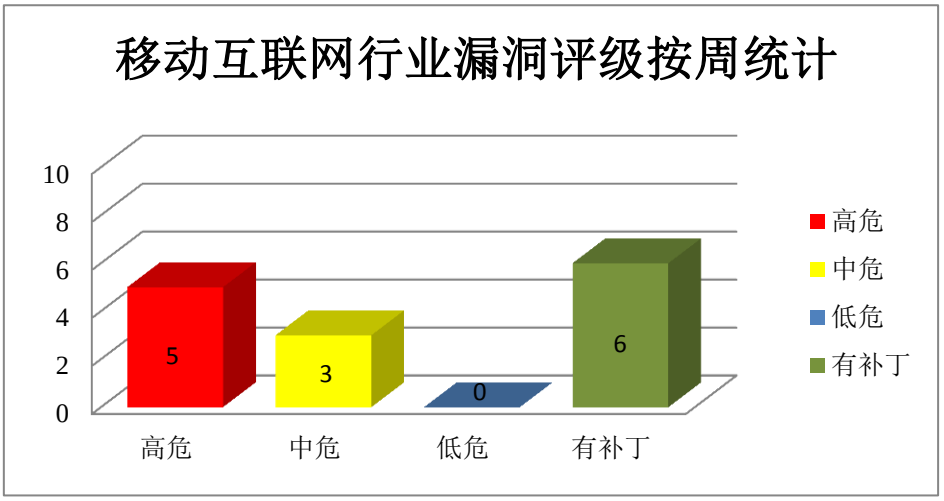

图 4 移动互联网行业漏洞统计

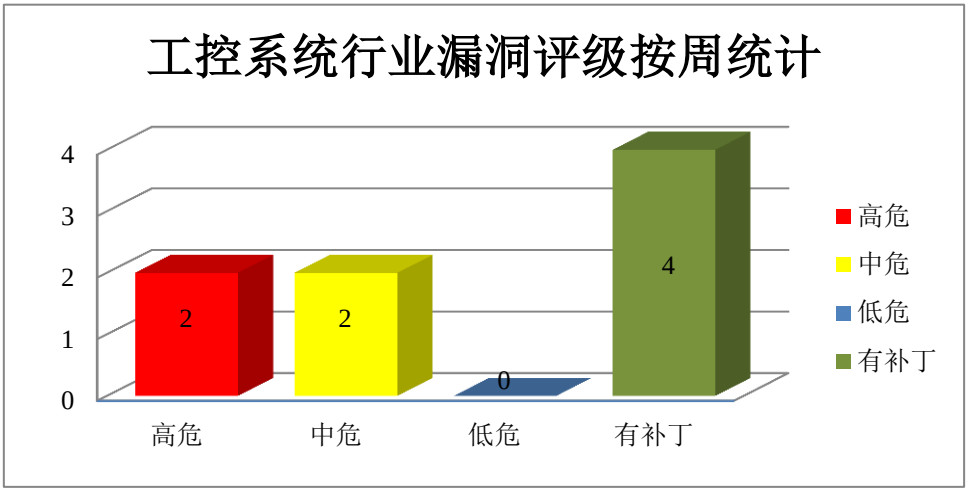

图 5 工控系统行业漏洞统计

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、Foxit 产品安全漏洞

Foxit Reader（旧名：Foxit PDF Reader）是一套用来阅读 PDF 格式文件的软件。PhantomPDF 是一个商业版。Foxit Reader 是一套自由使用的软件，操作系统主要以 Microsoft Windows 为主，且只要有 Win32 执行环境的操作系统上皆可使用。本周，上述产品被披露存在内存错误引用和类型混淆远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Foxit Reader 和 PhantomPDF 内存错误引用漏洞（CNVD-2018-14451）、Foxit Reader 类型混淆远程代码执行漏洞（CNVD-2018-14460、CNVD-2018-14461、CNVD-2018-14462、CNVD-2018-14463、CNVD-2018-14464、CNVD-2018-14465、CNVD-2018-14466）。其中，“Foxit Reader 和 PhantomPDF 内存错误引用漏洞（CNVD-2018-14451）”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-2018-14451

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14460

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14461

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14462

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14463

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14464

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14465

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14466

2、Cisco 产品安全漏洞

Cisco Firepower 4100 Series Next-Generation Firewalls 是一款 4100 系列的防火墙设备。FXOS Software 是一套运行在思科安全设备中的防火墙软件。NX-OS Software 是运行在思科交换机设备中的一套数据中心级操作系统软件。Cisco MDS 9000 Series Multilayer Switches 是一款 9000 系列的交换机设备。Nexus 2000 Series Fabric Extenders 是一款 Nexus 2000 系列交换阵列扩展器。Cisco Nexus 3000 和 9000 Series Switches 都是的不同系列的交换机设备。UCS 6200 Series Fabric Interconnects 是一套专用于 Cisco 设备的交换机矩阵。Firepower 9300 Security Appliance 是一款 9300 系列的安全设备。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，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：多款 Cisco 产品 FXOS Software 和 NX-OS Software Fabric Services 组件拒绝服务漏洞（CNVD-2018-14569、CNVD-2018-14571）、多款 Cisco 产品 NX-OS Software CLI 解析器输入验证漏洞、Cisco Nexus 4000 Series Switch NX-OS 输入验证漏洞、Cisco Nexus 3000 和 9000 Series Switches NX-OS 拒绝服务漏洞、多款 Cisco 产品 FXOS Software 和 UCS Fabric Interconnect Software CLI 解析器输入验证漏洞、多款 Cisco 产品 FXOS 和 UCS Fabric Interconnect Software 输入验证漏洞、Cisco Firepower 4100 Series Next-Generation Firewall 和 Firepower 9300 Security Appliance 路径遍历漏洞。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-2018-14569

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14571

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14570

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14576

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14579

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14580

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14577

http://www.cnvd.org.cn/flaw/show/CNVD-2018-14581

3、Samsung 产品安全漏洞

Samsung SmartThings Hub 是韩国三星（Samsung）公司的一款智能家居管理设备。video-core HTTP server 是其中的一个 HTTP 服务器。本周，上述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。

CNVD 收录的相关漏洞包括：Samsung SmartThings Hub video-core HTTP 服务器缓冲区溢出漏洞（CNVD-2018-14280、CNVD-2018-14281、CNVD-2018-14282、CNVD-2018-14283、CNVD-2018-14285、CNVD-2018-14284、CNVD-2018-14286、CNVD-2018-14287）。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-2018-14280
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14281
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14282
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14283
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14285
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14284
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14286
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14287

4、Adobe 产品安全漏洞

Adobe Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。本周，该产品被披露存在越界读取漏洞，攻击者可利用漏洞获取敏感信息。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 越界读取漏洞（CNVD-2018-14480、CNVD-2018-14481、CNVD-2018-14482、CNVD-2018-14483、CNVD-2018-14484、CNVD-2018-14485、CNVD-2018-14486、CNVD-2018-14489）。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-2018-14480
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14481
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14482
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14483
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14484
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14485
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14486
http://www.cnvd.org.cn/flaw/show/CNVD-2018-14489

5、PHPOK 任意文件上传漏洞

PHPOK 是一套支持扩展的企业建站系统。本周，PHPOK 被披露存在任意文件上传漏洞，攻击者可利用该漏洞上传任意的 zip 文件。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-2018-14359

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-2018-14152	Network Manager VPNC 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.gnome.org/GNOME/NetworkManager-vpnc
CNVD-2018-14213	Ffmpeg 缓冲区溢出漏洞（CNVD-2018-14213）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/FFmpeg/FFmpeg/commit/2b46ebdbff1d8dec7a3d8ea280a612b91a582869
CNVD-2018-14257	Advanced Order Export For WooCommerce 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://wordpress.org/plugins/woo-order-export-lite/#developers
CNVD-2018-14334	Sony IPELA E Series Camera measurementBitrateExec 功能命令注入漏洞	高	用户可联系供应商获得补丁信息：http://www.sony.com.cn/
CNVD-2018-14345	Symfony 认证绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://symfony.com/blog/cve-2018-11407-unauthorized-access-on-a-misconfigured-ldap-server-when-using-an-empty-password
CNVD-2018-14350	ZTE ZXIPTV-UCM 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：http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1008782
CNVD-2018-14455	WECON（维控）LeviStudioU 栈堆缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息：http://www.we-con.com.cn/download.aspx?id=13
CNVD-2018-14456	Davolink DVW-3200N 路由器弱密码漏洞	高	用户可联系供应商获得补丁信息：http://www.davolink.co.kr/sys/bbs/board.php?bo_table=0403&wr_id=50
CNVD-2018-14539	PGObject::Util::DBAdmin shell 代码注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/ledgersmb/PGObject-Util-DBAdmin
CNVD-2018-14584	SAP NetWeaver Instance Agent Service 内存破坏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://launchpad.support.sap.com/#/notes/2509284

小结：本周，Foxit 被披露存在内存错误引用和类型混淆远程代码执行漏洞，攻击者可利用漏洞执行任意代码。此外，Cisco、Samsung、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞攻击者可利用漏洞获取敏感信息，执行任意代码或发起拒绝服务攻击等。另外，PHPOK 存在任意文件上传漏洞，攻击者可利用该漏洞上传任意的

zip 文件。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. 三星智能家居平台 SmartThings Hub 出现大量漏洞

近期，安全研究人员在三星 SmartThings Hubs 中发现了 20 个漏洞。三星 SmaryThings Hub 是一个中央控制器，用于实时监控和管理物联网设备，包括相机、恒温器、LED 灯、智能插座、家庭报警系统以及运动探测器等，这些设备通过以太网、蓝牙 Zigbee 等多种技术链接。攻击者可利用这些漏洞进行 ddos 攻击和远程代码执行，达到完全的操控效果。

参考链接：https://www.helpnetsecurity.com/2018/07/27/samsung-smartthings-hub-vulnerabilities/

2. EOS 恶意合约可吞噬用户 RAM 漏洞

EOS，是专门为商用分布式应用而设计的一款高性能区块链操作系统，是一种新的区块链架构，旨在实现分布式应用的高性能扩展。EOS 的发布，被誉为区块链 3.0 时代的到来。本次发现的漏洞，恰好会导致用户账户内的 RAM 可能被恶意消耗，引发直接财产损失。恶意 EOS 合约存在吞噬用户 RAM 的安全风险，需要引起各大交易所、钱包、token 空投方、DApp、用户等的警惕，避免遭受损失。

参考链接：http://www.freebuf.com/vuls/179515.html

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