国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 04 月 03 日-2017 年 04 月 09 日 **2017 年第 15 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 135 个，其中高危漏洞 51 个、中危漏洞 63 个、低危漏洞 21 个。漏洞平均分值为 5.95。本周收录的漏洞中，涉及 0day 漏洞 39 个（占 29%），其中互联网上出现“Piwik 远程代码执行漏洞、WordPress 插件 Flash Rotator Gallery SQL 注入漏洞”零日代码攻击漏洞。此外，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 641 个，与上周（1119 个）环比下降 43%。

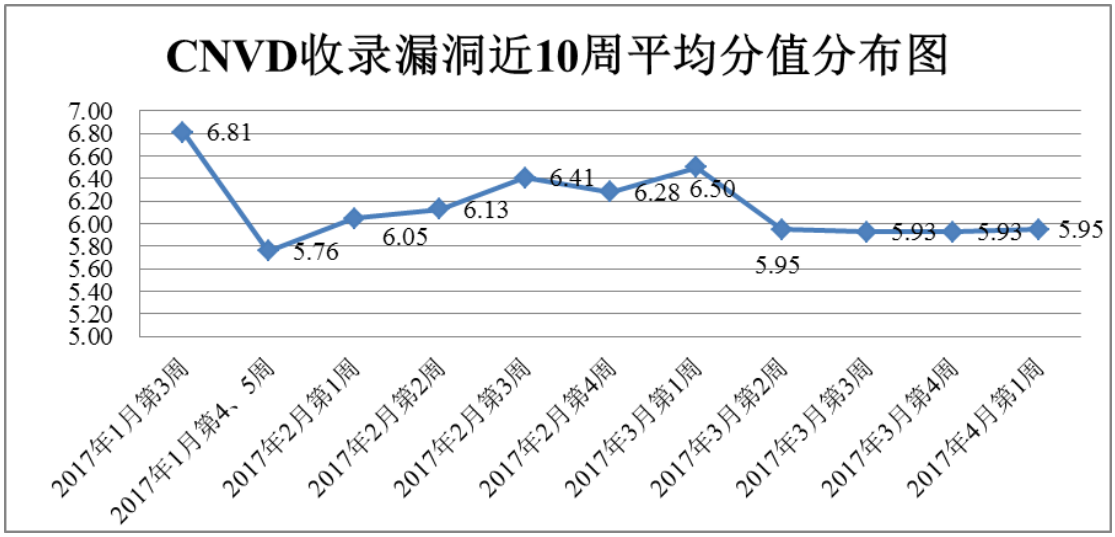

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 15 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 135 个漏洞。报送情况如表 1 所示。其中，安天实验室、华为技术有限公司、H3C、天融信等单位报送数量较多。漏洞盒子、广西鑫瀚科技有限公司、安徽新华博信息技术股份有限公司、上海零盾网络科技有限公司、江西安服信息产业有限公司、广州万方计算机

科技有限公司、广州神月信息安全技术有限公司、山东安云信息技术有限公司及其他个人白帽子向 CNVD 提交了 641 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
360 网神	249	249
安天实验室	112	0
华为技术有限公司	86	0
H3C	60	0
天融信	40	0
中国电信集团系统集成有限责任公司	36	0
绿盟科技	34	0
杭州安恒信息技术有限公司	29	0
安全狗	13	0
恒安嘉新	9	0
北京数字观星科技有限公司	5	0
北京启明星辰信息安全技术有限公司	3	3
深圳市深信服电子科技有限公司	3	3
西安四叶草信息技术有限公司	2	2
南京铱迅信息技术股份有限公司	1	1
漏洞盒子	209	209
广西鑫瀚科技有限公司	10	10
安徽新华博信息技术股份有限公司	10	10
上海零盾网络科技有限公司	8	8
江西安服信息产业有限公司	4	4

广州万方计算机科技有限公司	3	3
广州神月信息安全技术有限公司	3	3
山东安云信息技术有限公司	3	3
CNCERT 吉林分中心	4	4
CNCERT 北京分中心	2	2
CNCERT 湖南分中心	1	1
CNCERT 宁夏分中心	1	1
个人	125	125
报送总计	1065	641
录入总计	135（去重）	641

表 1 漏洞报送情况统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 135 个漏洞。其中应用程序漏洞 60 个，web 应用漏洞 32 个，操作系统漏洞 26 个，网络设备漏洞 15 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	60
web 应用漏洞	32
操作系统漏洞	26
网络设备漏洞	15
安全产品漏洞	2

表 2 漏洞按影响类型统计表

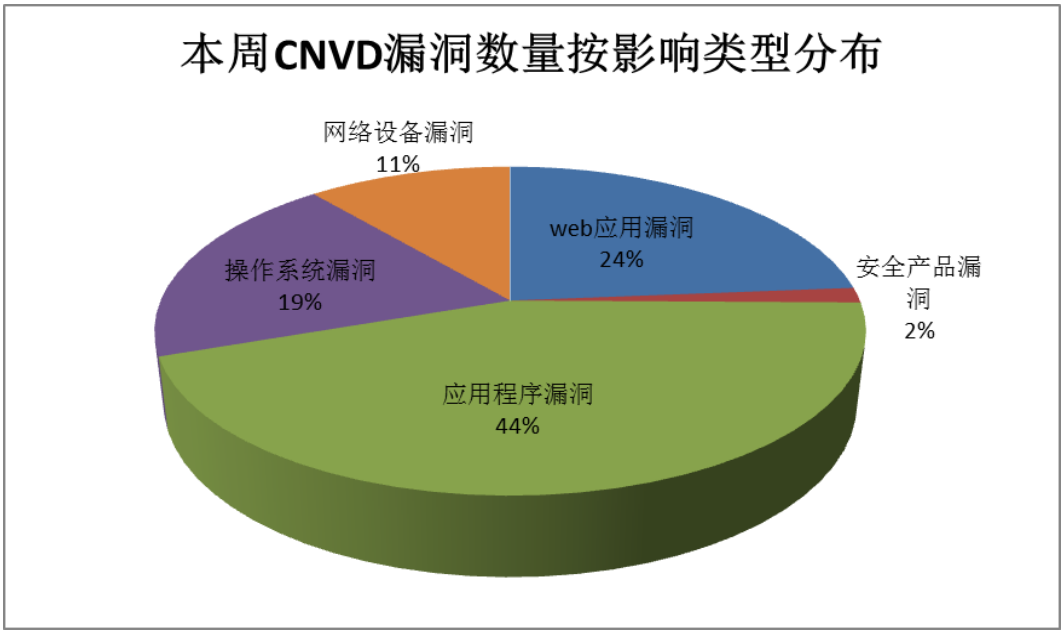

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Cisco、上海欧虎网络科技有限公司等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Google	17	13%
2	Cisco	12	10%
3	上海欧虎网络科技有限公司	10	7%
4	ImageMagick	9	7%
5	Microsoft	7	5%
6	Yxcms Inc.	6	4%
7	Gnome	3	2%
8	GNU	3	2%
9	Hikvision	3	2%
10	其他	65	48%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 5 个电信行业漏洞，23 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图所示）。其中，“Cisco IOS DHCP 拒绝服务漏洞、Cisco IOS XE Software L2TP 报文拒绝服务漏洞、Google Android Audioserver 权限提升漏洞（CNVD-20

17-03891）、Google Android Audioserver 权限提升漏洞（CNVD-2017-03890）、Google Nexus Kernel FIQ Debugger 特权提升漏洞”等的综合评级为“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/

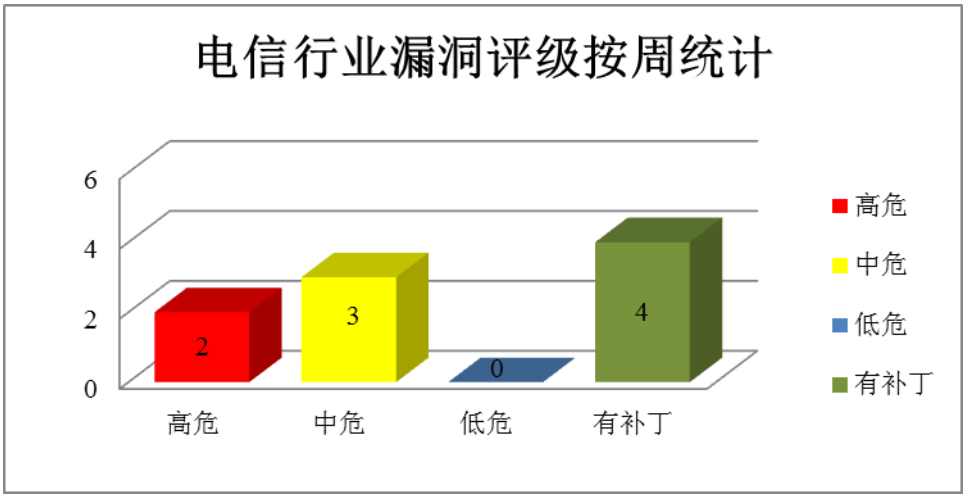

图 3 电信行业漏洞统计

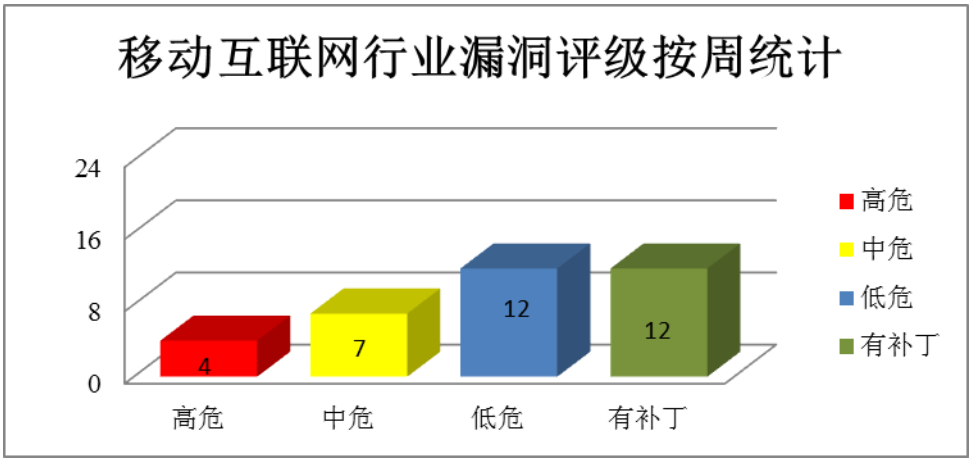

图 4 移动互联网行业漏洞统计

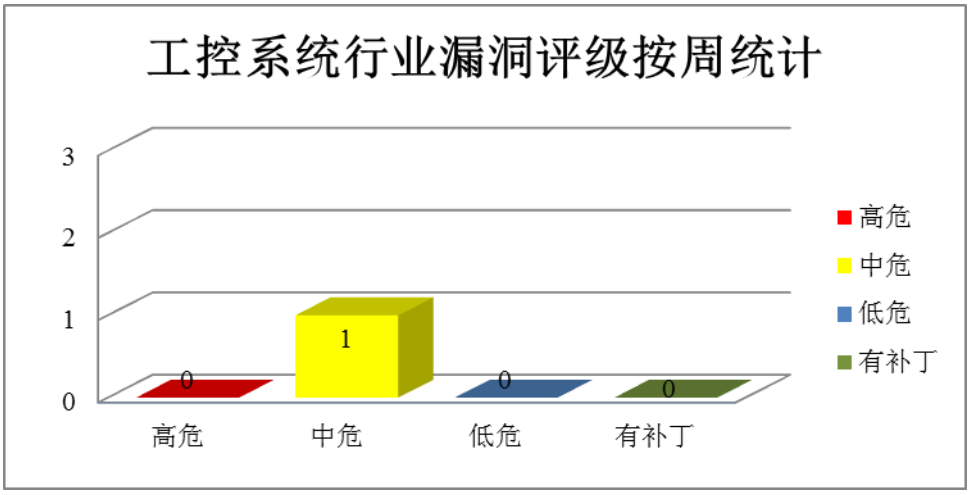

图 5 工控系统行业漏洞统计

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 IOS、Cisco IOx Software 和 IOS XE Software 都是美国思科公司为其网络设备开发的操作系统。Cisco Mobility Express 1800 Access Points 是基于 Mobility Express 解决方案的无线产品。Cisco Wireless LAN Controller 是一款无线局域网控制器。本周，上述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、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：Cisco IOS DHCP 拒绝服务漏洞、Cisco IOS XE Software L2TP 报文拒绝服务漏洞、Cisco IOS XE Software for Cisco ASR 920 Series Routers 拒绝服务漏洞、多个 Cisco 产品栈缓冲区溢出漏洞、Cisco IOS 和 IOS XE Software ANI IPv6 报文拒绝服务漏洞、Cisco IOS 和 IOS XE Software ANI 注册功能拒绝服务漏洞、Cisco Mobility Express 1800 Access Point Series 身份验证绕过漏洞、Cisco Wireless LAN Controller 远程安全绕过漏洞。除“Cisco IOS 和 IOS XE Software ANI 注册功能拒绝服务漏洞”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-2017-04006

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04004

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04003

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04002

http://www.cnvd.org.cn/flaw/show/CNVD-2017-03847

http://www.cnvd.org.cn/flaw/show/CNVD-2017-03848

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04106

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04111

2、Google 产品安全漏洞

Android 是美国谷歌公司和开放手持设备联盟共同开发的一套以 Linux 为基础的开源操作系统。Audioserver 是其中的一个音频服务器软件。Qualcomm SPCom Driver 是其中的一个串口通信驱动组件。Android on Nexus 9 是一套运行于 Nexus 9（平板电脑）中并以 Linux 为基础的开源操作系统。kernel FIQ debugger 是其中的一个内核调试器组件。本周，上述产品被披露存在权限提升和远程代码执行漏洞，攻击者可利用漏洞提升权限或远程执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Audioserver 权限提升漏洞（CNVD-2017-03891、CNVD-2017-03890）、Google Android Qualcomm SPCom 驱动程序远程代码执行漏洞、Google Nexus Kernel FIQ Debugger 特权提升漏洞、Google Android libgdx 远程代码执行漏洞（CNVD-2017-03885）、Google Android Framesequence Library 远程代码执行漏洞（CNVD-2017-03886）。其中“Google Android Audioserver 权限提升漏洞（CNVD-2017-03891、CNVD-2017-03890）、Google Nexus Kernel FIQ Debugger 特权提升漏洞”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-2017-03891

http://www.cnvd.org.cn/flaw/show/CNVD-2017-03890

http://www.cnvd.org.cn/flaw/show/CNVD-2017-03853

http://www.cnvd.org.cn/flaw/show/CNVD-2017-03878

http://www.cnvd.org.cn/flaw/show/CNVD-2017-03885

http://www.cnvd.org.cn/flaw/show/CNVD-2017-03886

3、Microsoft 产品安全漏洞

Microsoft Skype 是美国微软（Microsoft）公司的一套即时通讯软件。Microsoft Windows 是一系列操作系统。Hyper-V 是其中的一款虚拟化产品。Microsoft SharePoint Server 是一个服务器功能集成套件。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、远程执行任意代码和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Microsoft Skype DLL 加载本地代码执行漏洞、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2017-03849、CNVD-2017-03852）、Microsoft Windows Hyper-V 信息泄露漏洞、Microsoft Windows Hyper-V 拒绝服务漏洞（CNVD-2017-03851）、Microsoft XML Core Services 信息泄露漏洞（CNVD-2017-03862）、Microsoft SharePoint Server 跨站脚本漏洞（CNVD-2017-04008）。其中“Microsoft Skype DLL 加载本地代码执行漏洞、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2017-03849、CNVD-2017-03852）”的综合评级为“高危”。目前，厂商已经发

布了除“Microsoft Skype DLL 加载本地代码执行漏洞”外漏洞的修补程序。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-2017-04011
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03849
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03852
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03850
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03851
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03862
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04008

4、ImageMagick 产品安全漏洞

ImageMagick 是美国 ImageMagick Studio 公司的一套开源的图象处理软件。本周，该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或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：ImageMagick magick/cache.c 文件拒绝服务漏洞、ImageMagick xpm 文件拒绝服务漏洞、ImageMagick 'coders/tiff.c'文件拒绝服务漏洞、ImageMagick 任意命令执行漏洞、ImageMagick 整数溢出漏洞（CNVD-2017-03840）、ImageMagick 拒绝服务漏洞（CNVD-2017-03843、CNVD-2017-03844）、ImageMagick 内存破坏漏洞（CNVD-2017-03842）。其中，“ImageMagick 任意命令执行漏洞、ImageMagick 内存破坏漏洞（CNVD-2017-03842）”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-2017-03894
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03893
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03855
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03841
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03840
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03843
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03844
http://www.cnvd.org.cn/flaw/show/CNVD-2017-03842

5、三星 TiZen 系统存在多个高危漏洞

Tizen（泰泽）是两大 Linux 联盟 LiMo Foundation 和 Linux Foundation 整合资源优势，携手英特尔和三星电子，共同开发的一个开源的、标准化的基于 Linux 的操作系统。本周，三星 TiZen 系统被披露存在多个漏洞，攻击者可利用漏洞通过 Tizen Store 软件获取设备上的 root 权限并完全控制电视。目前，互联网上已经出现了针对该漏洞的攻击代码，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-2016-03991

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

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2017-03857	FFmpeg 'Libavcodec'远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://www.ffmpeg.org/security.html
CNVD-2017-03875	Disk Sorter Enterprise 'GET'缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接:http://www.disksorter.com/
CNVD-2017-03905	PHP FormMail Generator 任意代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.formmail-maker.com/generator.php
CNVD-2017-03898	Trend Micro SafeSync for Enterprise 存在多个漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.trendmicro.com/en_us/business.html
CNVD-2017-03897	Mozilla Firefox MFSA 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://www.mozilla.org/en-US/security/advisories/mfsa2017-05/
CNVD-2017-04005	Broadcom WiFi SoC 权限获取漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.broadcom.com/
CNVD-2017-04093	MagniComp Sysinfo 本地权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接:http://www.magnicomp.com/support/cve/CVE-2017-6516.shtml
CNVD-2017-04097	Apache POI 拒绝服务漏洞（CNVD-2017-04097）	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://poi.apache.org/
CNVD-2017-04109	AlienVault OSSIM 和 USM 身份验证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.alienvault.com/forums/discussion/7765/alienvault-v5-3-1-hotfix

表 4 部分重要高危漏洞列表

小结：本周，Cisco 被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制、执行任意代码或发起拒绝服务攻击等。此外，Gooole、Microsoft、ImageMagick 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、泄露敏感信息、提升权限或发

起拒绝服务攻击等。另外，三星 TiZen 系统被披露存在多个漏洞，攻击者可利用漏洞通过 Tizen Store 软件获取设备上的 root 权限并完全控制电视。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. Java AMF3 曝远程代码执行漏洞

近期，德国安全团队@codewhitesec 发现了 Java AMF3 的多个功能实现漏洞，美国 CERT/CC 也发出了安全预警。攻击者可以远程通过欺骗或控制服务连接方式，在 AMF 3 反序列动作时执行任意代码。CERT/CC 的安全公告提到了 3 个漏洞，第一个漏洞可让攻击者欺骗或控制 RMI（Remote Method Invocation）服务器来执行代码。第二个漏洞则可被攻击者利用实现任意代码执行——该漏洞影响到了 Flamingo，Apache 的 Flex BlazeDS 和 GraniteDS。XXE 漏洞也影响到了这些产品，另外还有 WebORB。

参考链接：http://www.freebuf.com/vuls/131335.html

2. 三星产品操作系统 Tizen 被曝存在 40 多个 0day 漏洞

在 4 月 3 日的卡巴斯基安全分析师峰会上，以色列安全研究人员 Amihai Neiderman 表示：三星产品主流操作系统 Tizen 存在 40 多个 0-day 漏洞，这些漏洞能让黑客非常容易远程攻击和控制三星设备，Neiderman 也计划陆续公布这些漏洞。目前，三星广泛在其智能电视、智能手表和 Z 系列智能手机中使用了 Tizen 操作系统，另外，为了减少对 Google Android 的依赖，三星还打算将其产品全面转移到 Tizen 系统上来。

参考链接：http://www.freebuf.com/news/131364.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：010-82990999