国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 01 月 11 日-2016 年 01 月 17 日 **2016 年第 3 期**

本周漏洞基本情况

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 118 个，其中高危漏洞 40 个、中危漏洞 59 个、低危漏洞 19 个。上述漏洞中，可利用来实施远程攻击的漏洞有 101 个。本周收录的漏洞中，已有 102 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。其中互联网上出现“Intel Network Adapter Diagnostic Driver 远程代码执行漏洞”等零日代码攻击漏洞，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 6 家成员单位、合作伙伴及个人报送了本周收录的全部 118 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、启明星辰、安天实验室、天融信等单位报送数量较多。补天平台、乌云、漏洞盒子、习科网络安全及白帽子向 CNVD 提交了 1018 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
奇虎(补天平台)	678	678
启明星辰	195	0
安天实验室	136	0
天融信	129	0
恒安嘉新	59	0
绿盟科技	53	0

H3C	4	0
乌云	271	271
漏洞盒子	37	37
High-Tech Bridge Security Research Lab	2	2
习科网络安全	1	1
CNCERT 宁夏分中心	2	2
个人	27	27
报送总计	1594	1018
录入总计	118（去重）	1018

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 IBM、Apple、Google 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	IBM	17	14%
2	Apple	13	11%
3	Google	13	11%
4	Adobe	7	6%
5	ownCloud	5	4%
6	TYPO3	4	3%
7	Proface	3	3%
8	Microsoft	2	2%
9	Cisco	2	2%
10	其他	53	44%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 118 个漏洞。其中应用程序漏洞 71 个，操作系统漏洞 19 个，网络设备漏洞 12 个，Web 应用漏洞 11 个，安全产品漏洞 4 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量

应用程序漏洞	71
操作系统漏洞	19
网络设备漏洞	12
Web 应用漏洞	11
安全产品漏洞	4
数据库漏洞	1

表 3 漏洞按影响类型统计表

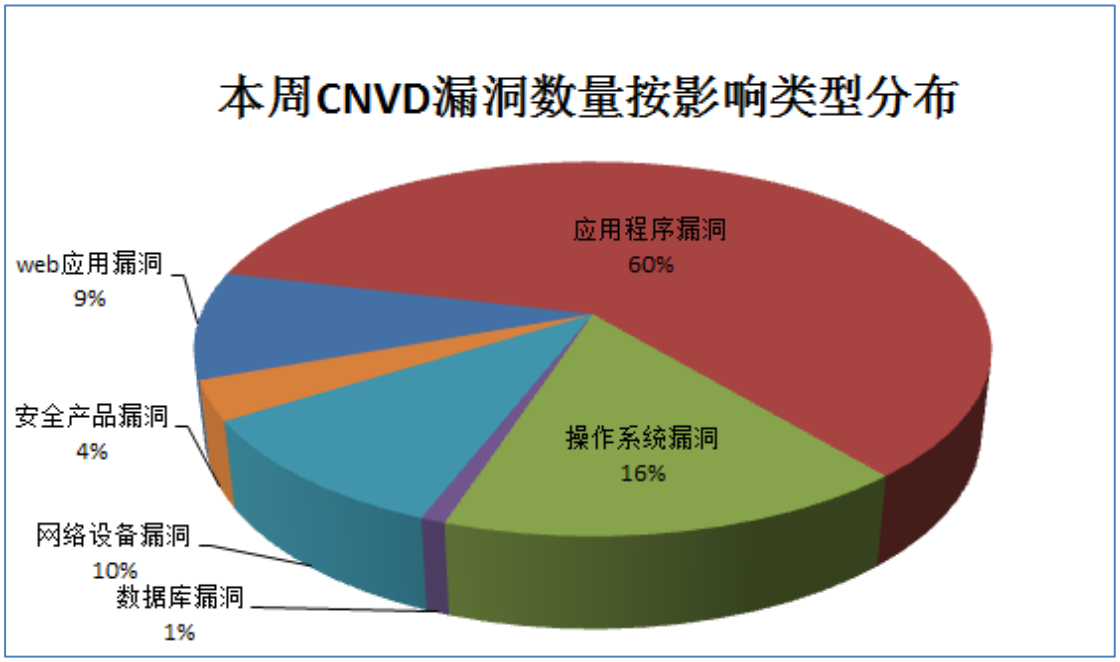

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 11 个电信行业漏洞、14 个移动互联网行业漏洞、4 个工控系统行业漏洞（如下图表所示）。其中，“Android Setup Wizard 权限提升漏洞、Android MediaTek misc-sd 权限提升漏洞、Android Imagination Technologies 权限提升漏洞、Android Trustzone 权限提升漏洞、Android kernel/sys.c 权限提升漏洞、Android Trustzone 权限提升漏洞（CNVD-2016-00122）、Android mediaserver 远程代码执行漏洞（CNVD-2016-00129）、Android kernel 信息泄露漏洞、Android System V IPC 拒绝服务漏洞、Apple iOS libxml2 内存破坏漏洞（CNVD-2016-00215）、Apple iOS libxml2 内存破坏漏洞、Unitronics VisiLogic OPLC IDE 缓冲区溢出漏洞”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。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2016-00127	PRTG 跨站脚本漏洞	中	否
电信	CNVD-2016-00147	Amped Wireless R10000 devices with firmware 欺骗漏洞	中	否

电信	CNVD-2016-00146	Amped Wireless R10000 devices with firmware 凭据管理漏洞	高	否
电信	CNVD-2016-00145	Amped Wireless R10000 devices with firmware 跨站请求伪造漏洞	中	否
电信	CNVD-2016-00152	ZyXEL NBG-418N devices with firmware 凭据管理漏洞	高	否
电信	CNVD-2016-00151	ZyXEL NBG-418N devices with firmware(AADZ.3)C0 跨站请求伪造漏洞	中	否
电信	CNVD-2016-00150	ReadyNet WRT300N-DD devices with firmware 授权问题漏洞	高	否
电信	CNVD-2016-00149	ReadyNet WRT300N-DD devices with firmware 欺骗漏洞	中	否
电信	CNVD-2016-00148	ReadyNet WRT300N-DD devices with firmware 跨站请求伪造漏洞	中	否
电信	CNVD-2016-00157	Cisco Unified Communications Manager SQL 注入漏洞	中	是
电信	CNVD-2016-00217	Blue Coat Systems ProxySG 和 Advanced Secure Gateway 开放重定向漏洞	低	是
移动互联网	CNVD-2016-00116	Android Bouncy Castle 信息泄露漏洞	中	是
移动互联网	CNVD-2016-00115	Android Setup Wizard 权限提升漏洞	高	是
移动互联网	CNVD-2016-00126	Android MediaTek misc-sd 权限提升漏洞	高	是
移动互联网	CNVD-2016-00125	Android Imagination Technologies 权限提升漏洞	高	是
移动互联网	CNVD-2016-00123	Android Trustzone 权限提升漏洞	高	是
移动互联网	CNVD-2016-00121	Android kernel/sys.c 权限提升漏洞	高	是
移动互联网	CNVD-2016-00118	Android Bluetooth 权限提升漏洞	低	是
移动互联网	CNVD-2016-00122	Android Trustzone 权限提升漏洞（CNVD-2016-00122）	高	是
移动互联网	CNVD-2016-00129	Android mediaserver 远程代码执行漏洞（CNVD-2016-00129）	高	是
移动互联网	CNVD-2016-00138	Android kernel 信息泄露漏洞	高	是
移动互联网	CNVD-2016-00136	Android System V IPC 拒绝服务漏洞	高	是
移动互联网	CNVD-2016-00140	Android SyncManager 拒绝服务漏洞	中	是
移动互联网	CNVD-2016-00215	Apple iOS libxml2 内存破坏漏洞（CNVD-2016-00215）	高	是
移动互联网	CNVD-2016-00216	Apple iOS libxml2 内存破坏漏洞	高	是
工控系统	CNVD-2016-00142	Unitronics VisiLogic OPLC IDE 缓冲区溢出漏洞	高	是
工控系统	CNVD-2016-00200	Proface GP-Pro EX D-Script 堆缓冲区溢出远程代码执行漏洞	中	否
工控系统	CNVD-2016-00201	Proface GP-Pro EX 越界读信息泄露漏洞	中	否
工控系统	CNVD-2016-00202	Proface GP-Pro EX 栈缓冲区溢出远程代码执行漏洞	中	否

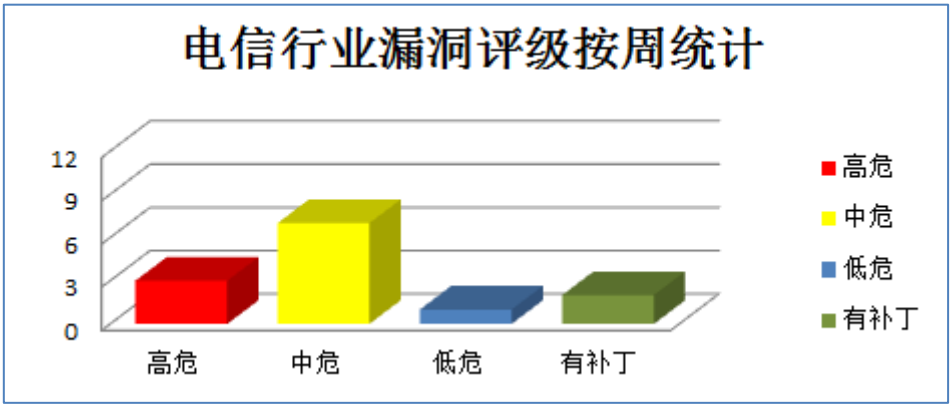

图 1 电信行业漏洞统计

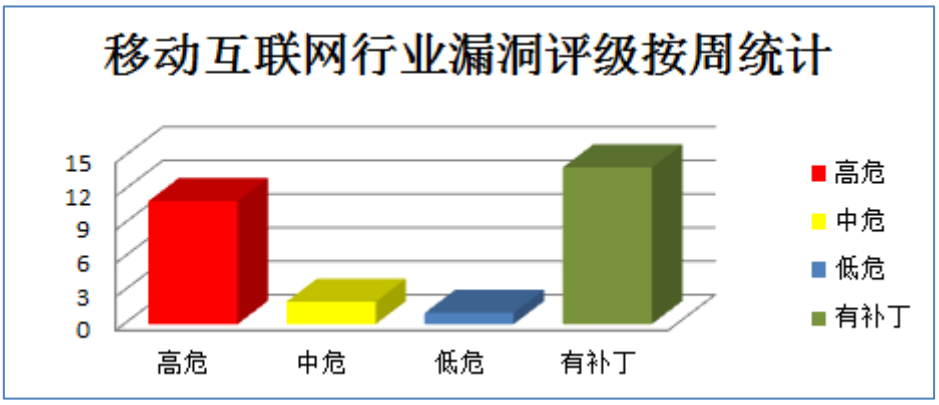

图 2 移动互联网行业漏洞统计

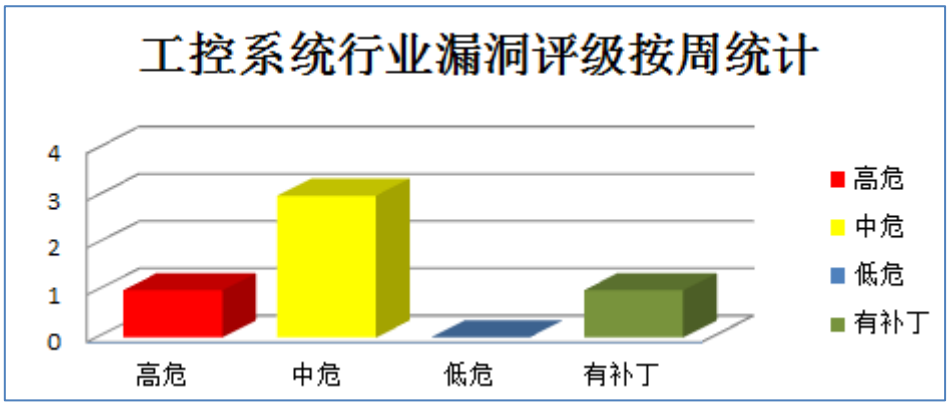

图 3 工控系统行业漏洞统计

本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、 Microsoft 产品安全漏洞

1 月 12 日，微软发布了 2016 年 1 月份月度例行安全公告，共含 9 项更新，修复了 MicrosoftWindows、Internet Explorer、Edge、Exchange Server、Office 和 Silverlight 中存在的 25 个安全漏洞。其中，6 项远程代码更新的综合评级为最高级“严重”级别。利

用上述漏洞，攻击者可提升权限，远程执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Vista SP2 Microsoft Windows Server 权限提升漏洞、Microsoft Windows Vista SP2 Microsoft Windows Server 权限提升漏洞（CNVD-C-2016-03500、CNVD-C-2016-03499、CNVD-C-2016-03493）、Microsoft Windows Vista SP2 Microsoft Windows Server 任意代码执行漏洞（CNVD-C-2016-03497）、Microsoft Windows Vista SP2 Microsoft Windows Server 任意代码执行漏洞、Microsoft Windows DLL 加载特权提升漏洞、Microsoft Edge 内存破坏漏洞。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了漏洞修补程序。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/webinfo/show/3774

2、 Fortigate 产品安全漏洞

本周，CNVD 收录了 Fortigate 防火墙存在 SSH 认证“后门”漏洞（CNVD-2016-00170）。远程攻击者可通过“后门”获取 Fortigate 防火墙系统的控制权限，进而渗透到内部网络区域，构成信息泄露和运行安全风险。

CNVD 收录的相关漏洞包括：Fortigate 防火墙存在 SSH 认证后门漏洞。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-2016-00170

3、 Oracle Glassfish 产品安全漏洞

本周，CNVD 收录了 GlassFish 存在任意文件读取漏洞（CNVD-2016-00232）。攻击者利用漏洞访问网站链接可获得非授权访问的目录文件列表，如:可读取 web 应用配置文件等，进一步渗透构成网站信息泄露和运行风险。

CNVD 收录的相关漏洞包括：GlassFish 任意文件读取漏洞。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-2016-00232

4、 Adobe 产品安全漏洞

Adobe Reader 是 PDF 文档阅读软件。本周，该产品被披露存在限制绕过和远程代码执行漏洞，攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Reader DC Global Javascript API 限制绕过漏洞、Adobe Reader JPEG2000 越界索引远程代码执行漏洞、Adobe Reader DC 远程代码执行漏洞、Adobe Reader DC 未初始化内存远程代码执行漏洞、Adobe Reader 内存错误远程代码执行漏洞、Adobe Reader DC AGM 远程代码执行漏洞（CNVD-2016-00227）。目前，厂商已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-2016-00222

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00223

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00224

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00225

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00226

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00227

5、ZyXEL NBG-418N devices with firmware 凭据管理漏洞

ZyXEL NBG-418N 是合勤（ZyXEL）科技公司的一款无线宽频路由器。本周，ZyXEL NBG-418N 被披露存在凭据管理漏洞，攻击者可利用漏洞通过局域网连接，以获得管理权限的默认密码。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-2016-00152

更多高危漏洞如表 3 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-2016-00130	AlienVault OSSIM 'assets[]'参数命令执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.alienvault.com/
CNVD-2016-00128	strongSwan 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，详情请关注厂商主页：https://www.strongswan.org/
CNVD-2016-00160	Ipswitch WhatsUp Gold SQL 注入漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：http://www.ipswitch.com/
CNVD-2016-00171	IBM Connections XML 解析拒绝服务漏洞	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-01.ibm.com/support/docview.wss?uid=swg21971439
CNVD-2016-00175	Apache Subversion 整数溢出漏洞	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://subversion.apache.org/security/CVE-2015-5259-advisory.txt
CNVD-2016-00174	Apache ActiveMQ 任意代码执行漏洞	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：http://activemq.apache.org/security-advisories.data/CVE-2015-5254-anno

			uncement.txt
CNVD-2016-00183	AVM FRITZ!OS 任意代码执行漏洞	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://avm.de/service/sicherheitsinfos-zu-updates/
CNVD-2016-00188	ownCloud Server 拒绝服务漏洞（CNVD-2016-00188）	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://owncloud.org/security/advisory/?id=oc-sa-2016-002
CNVD-2016-00186	Ruby colorscore gem 任意代码执行漏洞	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://rubygems.org/gems/colorscore
CNVD-2016-00206	Mozilla Firefox OS lockscreen 功能绕过漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://www.mozilla.org/en-US/security/advisories/mfsa2015-151/

表 3 部分高危漏洞列表

小结：本周，微软发布了 2016 年 1 月份的月度例行安全公告，共含 9 项更新，修复了多款产品中存在的 25 个安全漏洞。此外，Fortigate、GlassFish、Adobe 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获得权限、访问未授权目录文件和执行任意代码，同时由于相关攻击代码已经披露，近期预计将有较大规模的探测或攻击行为。此外，ZyXEL NBG-418N 被披露存在一个高危漏洞，攻击者可利用该漏洞通过局域网连接，以获得管理权限的默认密码。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。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Apache 修补 ActiveMQ/Subversion 产品漏洞

Apache ActiveMQ 是一套开源的消息中间件，支持 Java 消息服务、集群、Spring Framework 等。Apache Subversion 是一套开源的版本控制系统，该系统可兼容并发版本系统(CVS)。

本周，Apache 修补了上述产品存在的任意代码执行和整数溢出漏洞，避免攻击者利用漏洞执行任意代码。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。

补丁下载链接：http://www.cnvd.org.cn/patchInfo/show/69874

http://www.cnvd.org.cn/patchInfo/show/69873

本周要闻速递

1. 趋势科技杀毒软件被曝严重漏洞，黑客能够窃取你的所有密码

谷歌的 Project Zero 安全研究员 Tavis Ormandy 发现，趋势科技的杀毒软件的密码管理器组件中存在一个远程代码执行漏洞，允许黑客盗取用户的密码。目前，趋势科技已经发布了一个紧急补丁，以此来修复其杀毒软件产品中存在的几个严重漏洞。

参考链接：http://www.freebuf.com/news/93156.html

2. 谷歌 Play 商城又现恶意程序

近日，谷歌 Play 商城又现恶意程序。谷歌已从 Play 商城移除了 13 款含有“大脑测试程序”恶意病毒的应用程序。这款恶意程序应用会进行非授权下载，恶意为应用刷榜。

参考链接：http://www.freebuf.com/news/92602.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