国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 04 月 11 日-2016 年 04 月 17 日　　2016 年第 16 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 151 个，其中高危漏洞 66 个、中危漏洞 68 个、低危漏洞 17 个。漏洞平均分值为 5.92 分。本周收录的漏洞中，涉及 0day 漏洞 22 个（占 15%）。其中互联网上出现“Dell OpenManage Server Administrator 目录遍历漏洞、DotCMS 跨站脚本漏洞”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。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 758 个，与上周（742 个）环比持平。

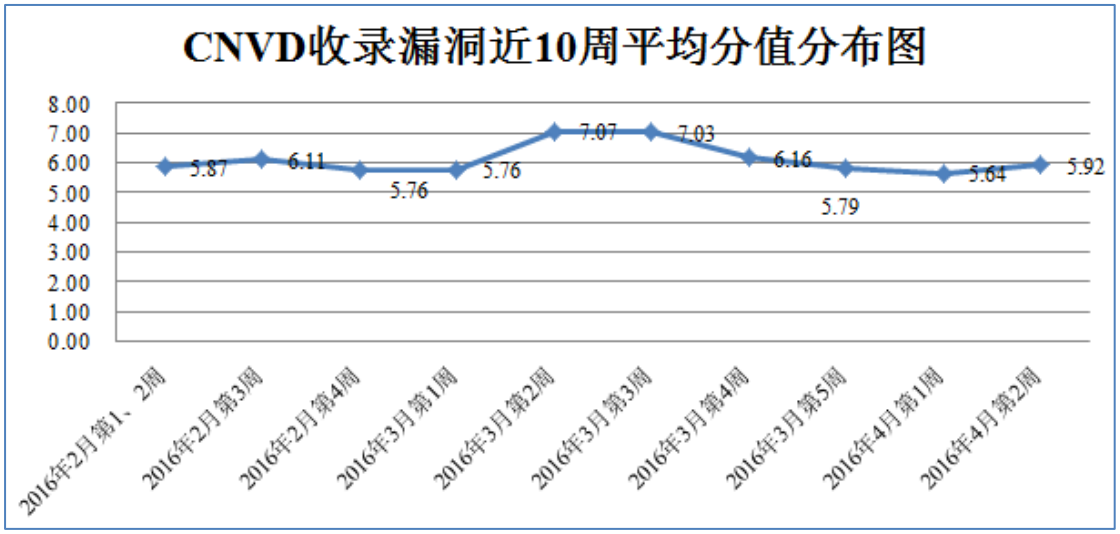

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 9 家成员单位、合作伙伴及个人报送了本周收录的全部 151 个漏洞。报送情况如表 1 所示。其中，天融信、安天实验室、启明星辰等单位报送数量较多。补天平台、乌云、漏洞盒子、腾讯玄武实验室、腾讯电脑管家、福建六壬网安股份有限公司、

河北翎贺计算机信息技术有限公司及白帽子向 CNVD 提交了 758 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
天融信	255	0
安天实验室	203	0
启明星辰	181	0
杭州安恒信息技术有限公司	102	0
奇虎(补天平台)	102	102
绿盟科技	64	0
恒安嘉新	63	2
东软	25	0
H3C	4	0
乌云	509	509
漏洞盒子	89	89
腾讯玄武实验室	12	12
腾讯电脑管家	9	9
福建六壬网安股份有限公司	2	2
河北翎贺计算机信息技术有限公司	1	1
CNCERT 福建分中心	1	1
个人	31	31
报送总计	1653	758
录入总计	151（去重）	758

表 1 成员单位上报漏洞统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 151 个漏洞。其中应用程序漏洞 115 个，操作系统漏洞 25 个，Web 应用漏洞 3 个，网络设备漏洞 3 个，安全产品漏洞 3 个、数据库漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	115
操作系统漏洞	25
Web 应用漏洞	3
网络设备漏洞	3
安全产品漏洞	3
数据库漏洞	2

表 2 漏洞按影响类型统计表

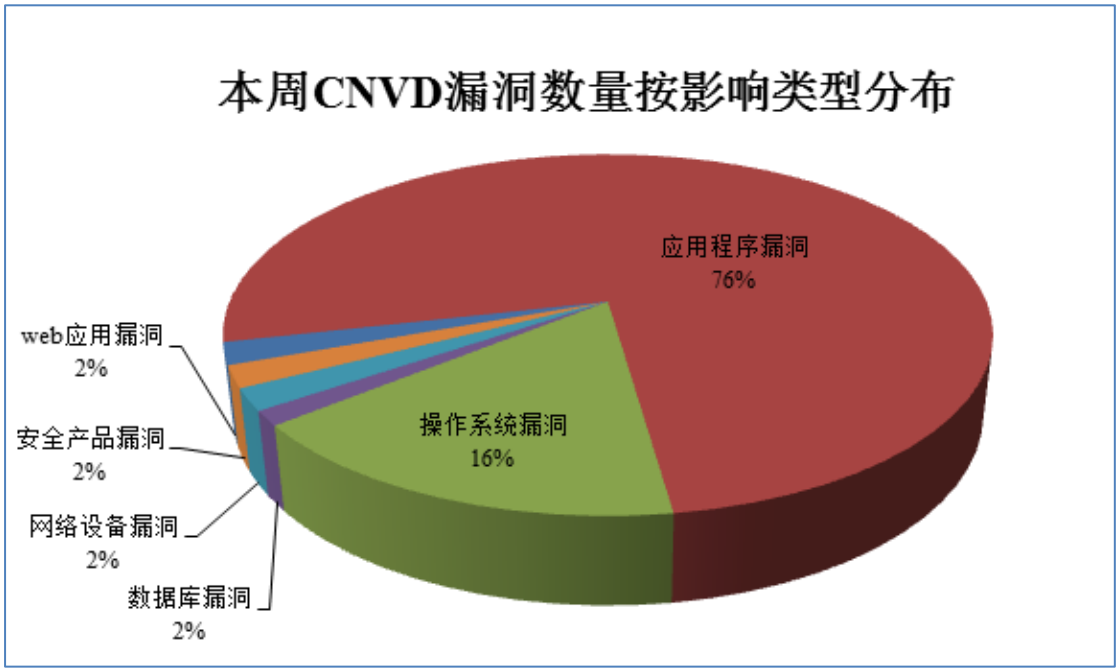

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、Silicon Graphics, Inc.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	Adobe	24	16%
2	Microsoft	20	13%
3	Silicon Graphics, Inc.	13	9%
4	Linux	9	6%
5	Google	8	5%
6	SAP	7	5%
7	IBM	6	4%
8	Apache	5	3%

9	Huawei	4	3%
10	其他	55	36%

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、7 个移动互联网漏洞、1 个工控系统行业漏洞（如下图所示）。其中，“华为 AR3200 设备输入校验漏洞”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/

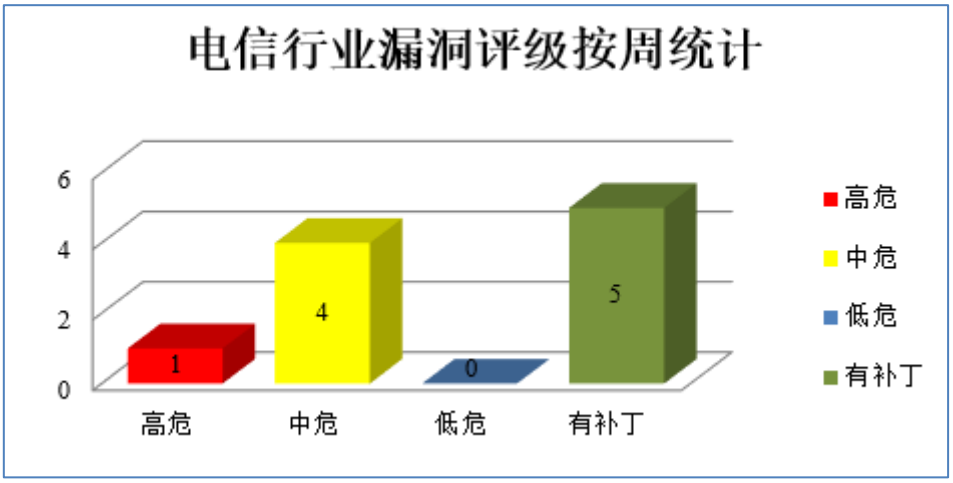

图 3 电信行业漏洞统计

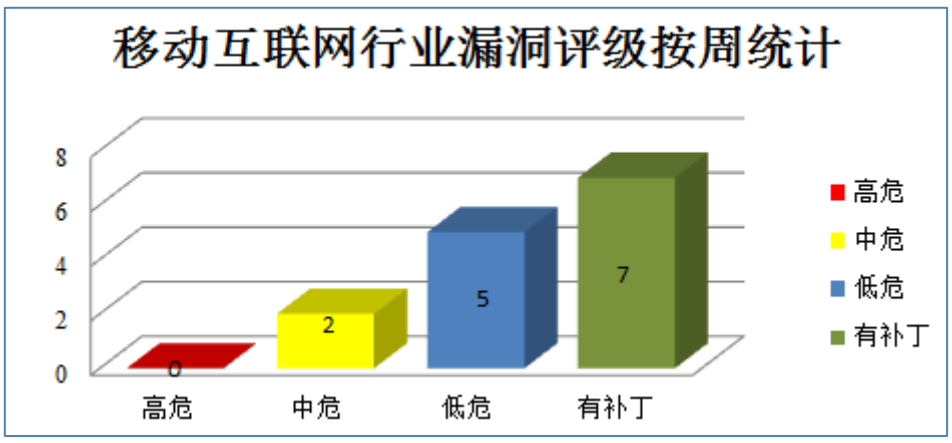

图 4 移动互联网行业漏洞统计

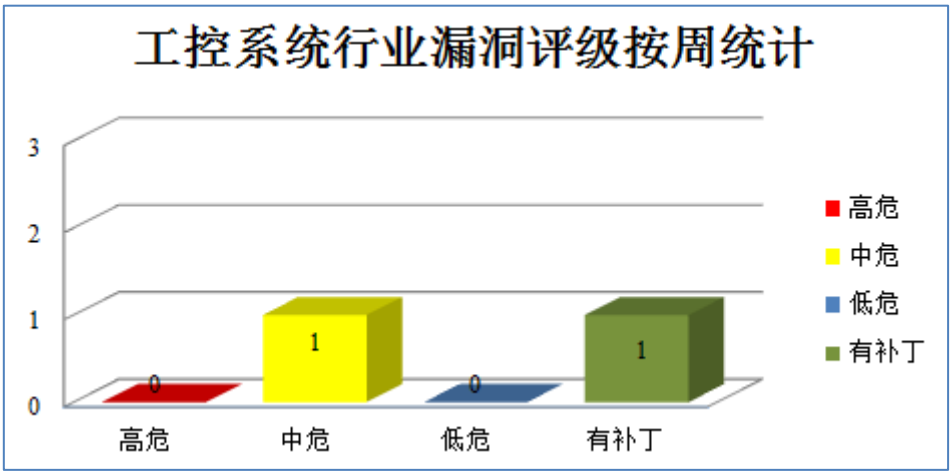

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

4 月 12 日，微软发布了 2016 年 4 月份的月度例行安全公告，共含 13 项更新，修复了 Microsoft Windows、Internet Explorer、Edge、.NET Framework、Office、Skype for Business、Microsoft Lync、Office Services 和 Web Apps、Flash Player 产品中存在的安全漏洞。其中，5 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 Edge 权限提升漏洞、Microsoft Edge 内存破坏漏洞（CNVD-2016-02218、CNVD-2016-02235、CNVD-2016-02236、CNVD-2016-02237）、Microsoft Office 内存破坏漏洞（CNVD-2016-02238、CNVD-2016-02239、CNVD-2016-02240）等。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/webinfo/show/3828

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，该产品被披露存在信息泄露、权限提升和拒绝服务漏洞，允许攻击者利用该漏洞获取敏感信息，提升权限和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Android Telephony 权限提升漏洞、Android SyncStorageEngine 拒绝服务漏洞、Android AOSP Mail 信息泄露漏洞、Android Qualcomm Video Kernel Driver 权限提升漏洞、Android Minikin 拒绝服务漏洞、Android Framework 组件信息泄露漏洞、Android BouncyCastle 信息泄露漏洞。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-2016-02118

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02119

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02120

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02121

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02122

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02123

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02124

3、 Adobe 产品安全漏洞

Adobe Flash Player 是一款跨平台、基于浏览器的多媒体播放器产品。本周，上述产品被披露存在内存破坏漏洞，允许攻击者利用漏洞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：Adobe Flash Player 内存破坏漏洞（CNVD-2016-02094、CNVD-2016-02095、CNVD-2016-02096、CNVD-2016-02098、CNVD-2016-02101、CNVD-2016-02102、CNVD-2016-02103、CNVD-2016-02104）等。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-2016-02094

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02095

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02096

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02098

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02101

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02102

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02103

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02104

4、 SAP 产品安全漏洞

SAP NetWeaver 是德国思爱普（SAP）公司的一套面向服务的集成化应用平台，该平台可为 SAP 应用提供开发和运行环境。SAP NetWeaver AS（Application Server）Java 是一款运行于 NetWeaver 中且基于 Java 编程语言的应用服务器。Internet Communication Manager（又名 ICMAN 或 ICM）是其中的一个通信管理器组件。本周，该产品被披露存在多个漏洞，允许攻击者可利用漏洞注入任意 Web 脚本或 HTML、造成拒绝服务和读取任意文件等。

CNVD 收录的相关漏洞包括：SAP NetWeaver AS JAVA Internet Communication Manager 组件拒绝服务漏洞、SAP NetWeaver AS JAVA Java Startup Framework 组件拒绝服务漏洞、SAP NetWeaver Java AS 目录遍历漏洞、SAP NetWeaver Java AS XML

DAS 漏洞、SAP NetWeaver Java AS RTC 服务信息泄露漏洞、SAP NetWeaver Java AS XXE 漏洞、SAP NetWeaver Java AS 跨站脚本漏洞。其中，“SAP NetWeaver AS JAVA Internet Communication Manager 组件拒绝服务漏洞、SAP NetWeaver AS JAVA Java Startup Framework 组件拒绝服务漏洞”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-2016-02186

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02185

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02126

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02128

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02129

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02130

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02131

5、 Linux kernel ‘mark_source_chains()’拒绝服务漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，Linux kernel 被披露存在拒绝服务漏洞，允许攻击者利用漏洞发起拒绝服务攻击。目前，厂商尚未发布该漏洞的修补程序。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-2016-02152

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-2016-02140	OAR 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：https://www.debian.org/security/2016/dsa-3543
CNVD-2016-02143	Lemur Vehicle Monitors BlueDriver 安全绕过漏洞	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.lemurmonitors.com/
CNVD-2016-02142	PuTTY 和 KiTTY 栈缓冲区溢出漏洞	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.chiark.greenend.org.uk/~sgtatham/putty/
CNVD-2016-02170	OptiPNG 内存错误引用漏洞	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.debian.org/security/2016/dsa-3546
CNVD-2016-02168	Lenovo Fingerprint Manager 和 Touch Fingerprint 权限获取漏洞	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://support.lenovo.com/us/en/product_security/len_4282
CNVD-2016-02162	Huawei Policy Center SQL 注入漏洞	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.huawei.com/en/psirt/security-advisories/huawei-sa-20160325-01-policycenter-en
CNVD-2016-02158	Foreman 未授权操作漏洞	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://theforeman.org/security.html#CVE-2015-5233:reportsshow/destroynotrestrictedbyhostauthorization
CNVD-2016-02171	OptiPNG 内存错误引用漏洞（CNVD-2016-02171）	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.debian.org/security/2016/dsa-3546
CNVD-2016-02175	Silicon Graphics LibTiff 拒绝服务漏洞	高	暂无
CNVD-2016-02176	F5 BIG-IP APM 和 BIG-IP Edge Gateway 未授权访问漏洞	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://support.f5.com/kb/en-us/solutions/public/k/82/sol82679059.html

表 4 部分重要高危漏洞列表

小结：4 月 12 日，微软发布了 2016 年 4 月份的月度例行安全公告，共含 13 项更新，修复了 Microsoft Windows、Internet Explorer、Edge、.NET Framework、Office、Skype for Business、Microsoft Lync、Office Services 和 Web Apps、Flash Player 产品中存在的安全漏洞。其中，5 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。此外，Google、Adobe、SAP 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码、获取敏感信息、提升权限、注入任意 Web 脚本或 HTML 或发起拒绝服务攻击等。另外，Linux kernel 被披露存在一个高危漏洞，允许攻击者利用漏洞发起拒绝服务攻击。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

安全预警：全球 1.35 亿的 ARRIS 有线调制解调器可被远程攻击

ARRIS SURFboard 的有线调制解调器中被发现一枚安全漏洞，攻击者可远程攻击全球约 1.35 亿的设备。安全专家 David Longenecker 解释：ARRIS（前身是 Motorola）生产的一款非常流行的有线调制解调器中存在一个安全漏洞，影响数十亿设备。这款 ARRIS SB6141 售价约 70 美元，150 兆的网速，被美国网络供应商们广泛使用。攻击者

可利用 ARRIS SURF 解调器中的漏洞远程攻击设备，并控制设备长达三十分钟。

参考链接：http://www.freebuf.com/news/101244.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