

信息安全漏洞周报

2016 年 03 月 07 日-2016 年 03 月 13 日

2016 年第 11 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**高**。

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 119 个，其中高危漏洞 68 个、中危漏洞 46 个、低危漏洞 5 个。漏洞平均分为 7.07 分。本周收录的漏洞中，涉及 0day 漏洞 8 个（占 7%）。本周，Apache Jetspeed 以及 ISC BIND 等广泛应用的 WEB、DNS 系统软件存在高危漏洞，可对域名解析系统以及大量的 Web 服务器构成拒绝服务或远程控制安全风险，同时本周也是微软例行的安全补丁周，用户需要及时更新补丁。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 1214 个，与上周（1945 个）环比下降 38%。

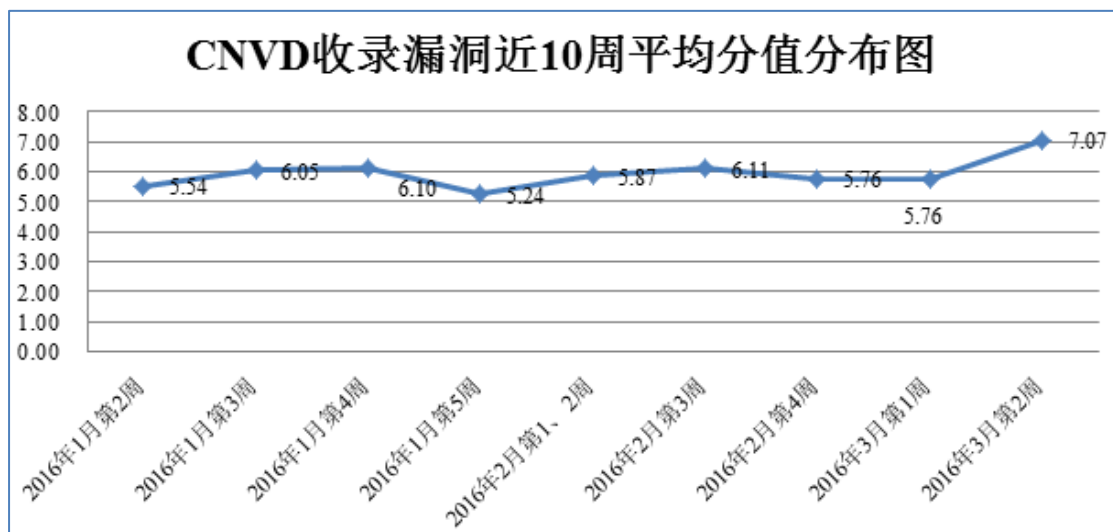


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 7 家成员单位、合作伙伴及个人报送了本周收录的全部 119 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、深圳市深信服电子科技有限公司、广州白狐网络科技有限公司及白帽子向 CNVD 提交了 1214 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)	596	596
启明星辰	223	0
安天实验室	118	0
天融信	101	0
恒安嘉新	80	0
绿盟科技	49	0
H3C	4	0
乌云	530	530
漏洞盒子	31	31
深圳市深信服电子科技有限公司	1	1
广州白狐网络科技有限公司	1	1
西安四叶草信息技术有限公司	1	1
CNCERT 安徽分中心	3	3
CNCERT 福建分中心	2	2
个人	49	49
报送总计	1789	1214
录入总计	119（去重）	1214

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 119 个漏洞。其中应用程序漏洞 88 个，操作系统漏洞 16 个，网络设备漏洞 10 个，Web 应用漏洞 4 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	88
操作系统漏洞	16
网络设备漏洞	10
Web 应用漏洞	4
安全产品漏洞	1

表 2 漏洞按影响类型统计表

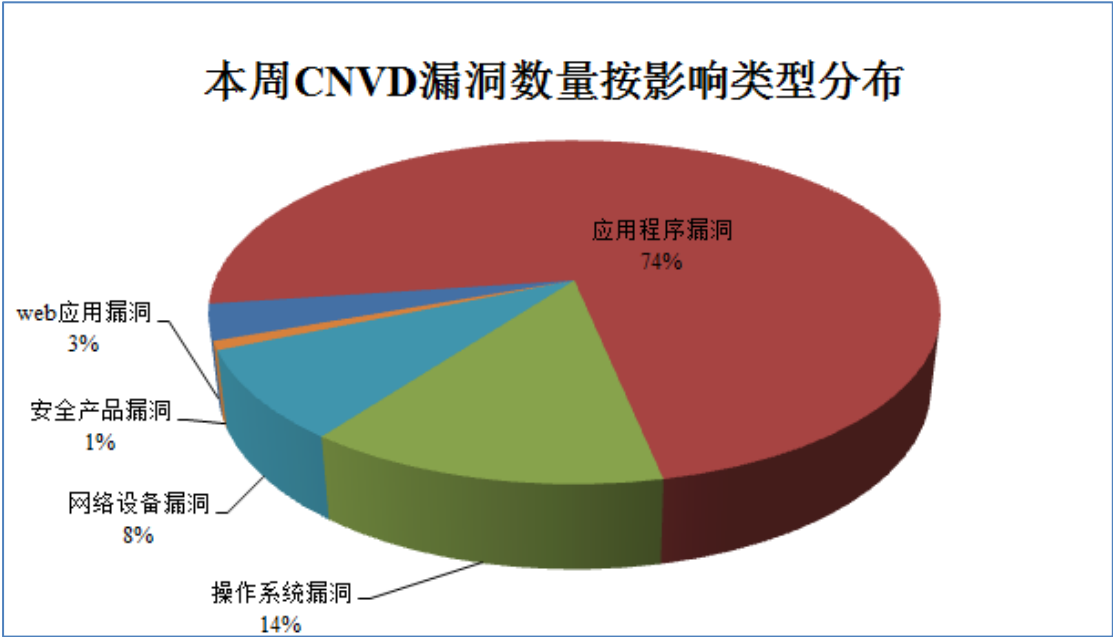


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Google、Adobe 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	Microsoft	40	34%
2	Google	21	18%
3	Adobe	13	11%
4	Cisco	11	9%
5	HP	4	3%
6	OpenSSL	3	3%
7	ISC, Inc.	3	3%
8	Apache	2	2%
9	IBM	2	2%
10	其他	20	15%

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、4 个工控系统行业漏洞（如下图所示）。其中，“HP Network Automation 存在多个漏洞、HP Network Automation 存在多个漏洞（CNVD-2016-01552）、Google Nexus Bluetooth 组件拒绝服务漏洞、Google Nexus mediaserver 内存破坏漏洞、ISC BIND DNAME 解析记录签名校验拒绝服务漏洞、Cisco NX-OS Software 拒绝服务漏洞（CNVD-2016-01460、CNVD-2016-01459）、Cisco Nexus 3000/3500 交换机默认凭证漏洞”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/>

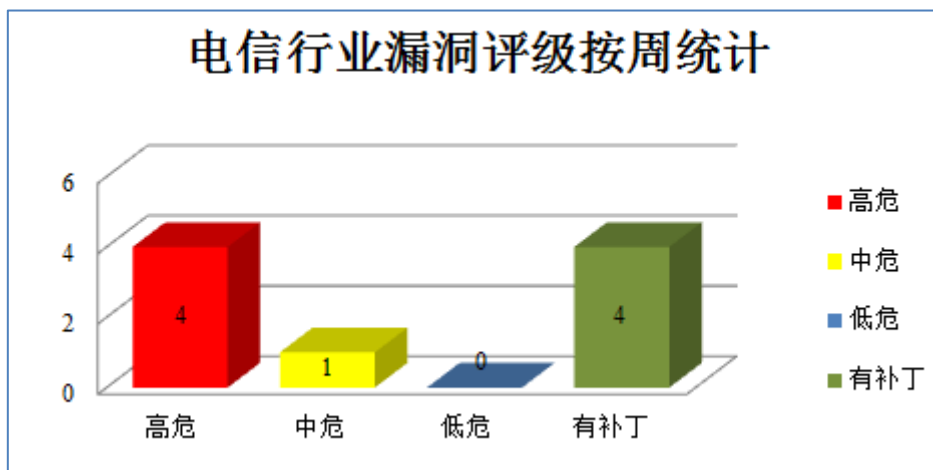


图 3 电信行业漏洞统计

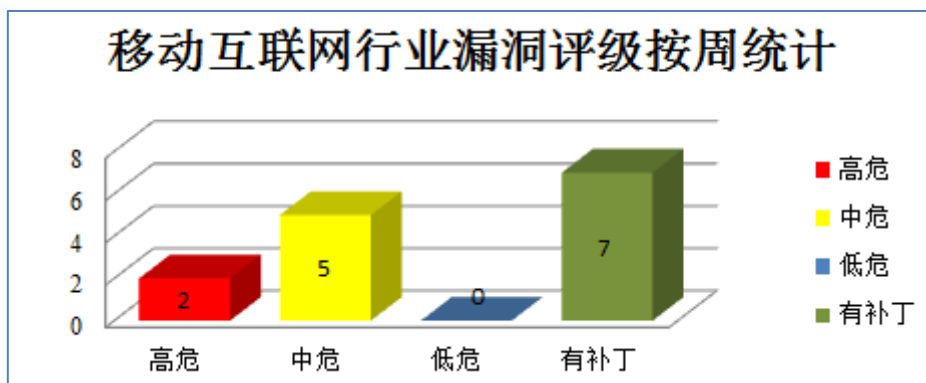


图 4 移动互联网行业漏洞统计

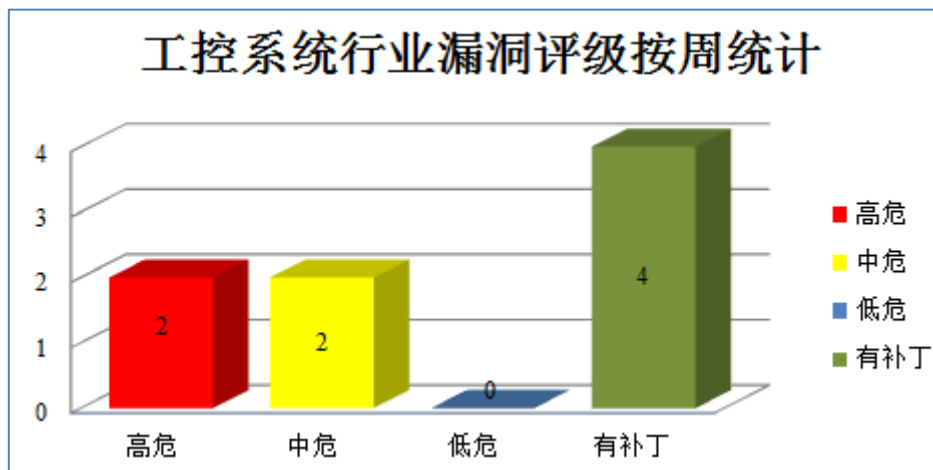


图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

3月8日，微软发布了2016年3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、Server、Office、Office Service、Web Apps、和.NET Framework中存在的44个安全漏洞。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 Internet Explorer 内存破坏漏洞（CNVD-2016-01576、CNVD-2016-01575、CNVD-2016-01590、CNVD-2016-01529、CNVD-2016-01531、CNVD-2016-01537、CNVD-2016-01501）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/3808>

2、Apache 产品安全漏洞

Jetspeed 是基于 Java 和 XML 的开源的企业信息门户的实现。Jetspeed 可集成各种数据源，通过 XSL 技术将数据组织成 Jsp 页面或 Html 页面传给客户端；Jetspeed 还支持模板和内容的发布框架。本周，上述产品被披露存在目录穿越漏洞和未授权访问漏洞，远程攻击者可利用漏洞通过调用 REST API 来管理系统用户，并在拥有管理员权限账号的情况下，上传任意文件，进而导致远程命令执行。

CNVD 收录的相关漏洞包括：Apache Jetspeed 目录穿越漏洞、Apache Jetspeed 用户管理 REST API 未授权访问漏洞。上述漏洞的综合评级为“高危”。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-2016-01499>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01500>

3、ISC 产品安全漏洞

ISC BIND 是一套实现了 DNS 协议的开源软件。本周, 上述产品被披露存在拒绝服务漏洞, 远程攻击者可利用上述漏洞, 可发起拒绝服务攻击, 对互联网上广泛应用 BIND 系统解析软件的域名服务器构成安全运行风险。

CNVD 收录的相关漏洞包括:ISC BIND DNAME 解析记录签名校验拒绝服务漏洞、ISC BIND rndc 控制实例拒绝服务漏洞、ISC BIND 查询包 cookie 选项拒绝服务漏洞。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-2016-01548>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01549>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01550>

4、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。Blink 是美国谷歌 (Google) 公司和挪威欧朋 (Opera Software) 公司共同开发的一套浏览器排版引擎 (渲染引擎)。本周, 该产品被披露存在拒绝服务、内存错误引用和安全绕过漏洞, 攻击者利用漏洞可绕过安全限制、执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括: Google Chrome Blink 拒绝服务漏洞 (CNVD-2016-01503)、Google Chrome V8 拒绝服务漏洞 (CNVD-2016-01508)、Google Chrome 内存错误引用漏洞 (CNVD-2016-01504)、Google Chrome WebRTC Audio Private API 内存错误引用漏洞、Google Chrome 安全绕过漏洞 (CNVD-2016-01515)、Google Chrome 拒绝服务漏洞 (CNVD-2016-01509)、Google Chrome Blink 内存错误引用漏洞 (CNVD-2016-01514、CNVD-2016-01510) 等。上述漏洞的综合评级均为“高危”。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-2016-01503>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01508>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01504>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01505>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01515>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01509>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01514>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01510>

5、SAP 3D Visual Enterprise Viewern 内存错误引用远程代码执行漏洞（CNVD-2016-01564）

SAP 3D Visual Enterprise Viewer（VEV）是德国思爱普（SAP）公司的一套用于查看、缩放、平移和旋转交互式三维数据以及播放分步动画的软件。本周，SAP 3D Visual Enterprise Viewernr 被披露存在内存错误引用远程代码执行漏洞，攻击者可利用漏洞执行任意代码。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-2016-01564>

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-2016-01462	OpenSSL BN_hex2bn/BN_dec2bn 空指针间接引用及堆破坏漏洞	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.openssl.org/news/secadv/20160301.txt
CNVD-2016-01476	Exim Configuration File Path 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://lists.exim.org/lurker/message/20160302.191005.a72d8433.en.html
CNVD-2016-01479	OpenSSL 拒绝服务漏洞（CNVD-2016-01479）	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://openssl.org/news/secadv/20160301.txt
CNVD-2016-01482	BeanShell 任意命令执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.debian.org/security/2016/dsa-3504
CNVD-2016-01518	Adobe Flash MPEG-4 越界读远程代码执行漏洞（CNVD-2016-01518）	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://helpx.adobe.com/security/products/flash-player/apsb15-32.html
CNVD-2016-01519	Adobe Flash MPEG-4 越界读远程代码执行漏洞（CNVD-2016-01519）	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://helpx.adobe.com/security/products/flash-player/apsb15-32.html
CNVD-2016-01521	Adobe Flash MPEG-4 内存错误引用远程代码执行漏洞	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://helpx.adobe.com/security/products/flash-player/apsb15-32.html

CNVD-2016-01525	Adobe Flash MPEG-4 内存错误引用远程代码执行漏洞 (CNVD-2016-01525)	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://helpx.adobe.com/security/products/flash-player/apsb15-32.html
CNVD-2016-01539	多款 Adobe 产品任意代码执行漏洞 (CNVD-2016-01539)	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://helpx.adobe.com/security/products/acrobat/apsb16-09.html
CNVD-2016-01561	PHP PHAR 'ext/phar/tar.c'栈缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://www.php.net/

表 4 部分重要高危漏洞列表

小结：本周，微软发布了 2016 年 3 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、Server、Office、Office Service、Web Apps、和 .NET Framework 中存在的 44 个安全漏洞。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，Apache、ISC、Google 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绕过安全限制、执行任意代码、上传任意文件或发起拒绝服务攻击等。此外，SAP 3D Visual Enterprise Viewer (VEV) 被披露存在一个内存错误引用远程代码执行漏洞，攻击者可利用该漏洞执行任意代码。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。

本周漏洞要闻速递

1. SpagoBI 的远程代码执行漏洞

SpagoBI 是一款免费开源商务智能套件，其由 Engineering Group 的 SpagoBI 实验室 (www.eng.it) SpagoBI 实验室开发和管理。SpagoBI 使用 Groovy 库在后端完成一些动态商业智能套件的操作。从源代码我们可以看到有后端有几个部分是用来解析输入的内容。Groovy 支持本地 Java 对象，所以如果在这些地方没有过滤的话就很容易导致代码执行。实际上在该系统中，并没有对输入进行过滤，Groovy 库中存在几个滥用的函数，攻击者可通过控制输入执行任意代码。

参考链接：<http://www.freebuf.com/news/98450.html>

2. 微软“WebDAV”提权漏洞

微软官方描述：如果 Microsoft Web 分布式创作和版本管理 (WebDAV) 客户端验证输入不当，那么其中就会存在特权提升漏洞。成功利用此漏洞的攻击者可以使用提升的特权执行任意代码。若要利用此漏洞，攻击者首先必须登录系统。然后，攻击者可以运行一个为利用此漏洞而经特殊设计的应用程序，从而控制受影响的系统。工作站和服

务器最易受此攻击威胁。此安全更新程序通过更正 WebDAV 验证输入的方式来修复这个漏洞。且微软介绍，此漏洞是一个限定系统的提权漏洞，因为此漏洞在 win8 或者更高的系统上是触发 BSOD，而在 win7 及以下的系统中才能提权成功。所以微软设定此漏洞的安全等级为：中。

参考链接：<http://www.freebuf.com/vuls/98486.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