

信息安全漏洞周报

2016 年 02 月 01 日-2016 年 02 月 14 日

2016年第6、7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**低**。

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 101 个，其中高危漏洞 24 个、中危漏洞 71 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 93 个。本周收录的漏洞中，已有 97 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“用友 ICC 系统任意文件上传漏洞”等零日漏洞，涉及国内较多企事业单位用户，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 101 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、天融信、启明星辰、安天实验室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 804 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)	534	534
天融信	182	0
启明星辰	153	0
安天实验室	148	0
H3C	5	0

恒安嘉新	11	0
乌云	237	237
漏洞盒子	7	7
习科网络安全	1	1
CNCERT 宁夏分中心	1	1
个人	24	24
报送总计	1303	804
录入总计	101（去重）	804

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、Cisco、NTP 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	Google	12	12%
2	Cisco	9	9%
3	NTP	7	7%
4	IBM	6	6%
5	phpMyAdmin	6	6%
6	Mozilla	5	5%
7	FreeBSD	4	4%
8	Oracle	4	4%
9	OpenSSL	2	2%
10	其他	46	45%

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 101 个漏洞。其中应用程序漏洞 79 个，网络设备漏洞 12 个，操作系统漏洞 4 个，Web 应用漏洞 3 个，安全产品 2 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	79
网络设备漏洞	12

操作系统漏洞	4
Web 应用漏洞	3
安全产品漏洞	2
数据库漏洞	1

表 3 漏洞按影响类型统计表

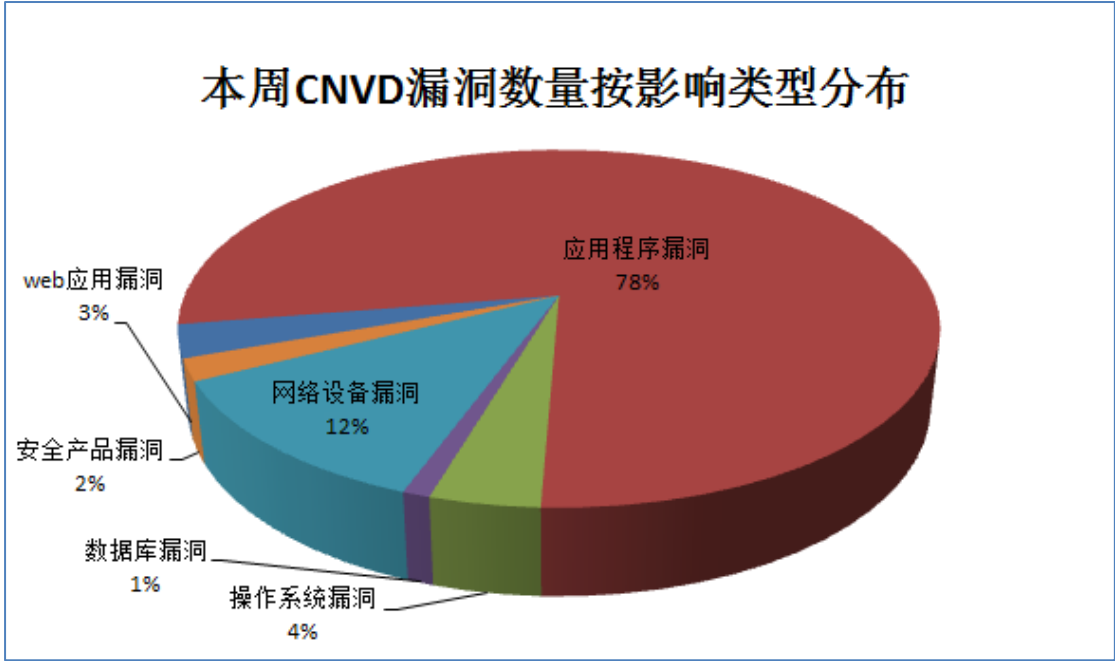


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 8 个电信行业漏洞、2 个移动互联网行业漏洞、3 个工控系统行业漏洞（如下图表所示）。其中，“Cisco RV220W SQL 注入漏洞、MICROSYS PRO MOTIC 堆缓冲区溢出漏洞、Rockwell Automation MicroLogix 1100 PLC 栈缓冲区溢出漏洞”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-2016-00768	IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2016-00768）	低	是
电信	CNVD-2016-00775	多款 Buffalo 设备跨站请求伪造漏洞	低	是
电信	CNVD-2016-00774	Samsung Note 3 和 Galaxy S6 拒绝服务漏洞	中	否
电信	CNVD-2016-00788	Cisco Small Business SG300 拒绝服务漏洞	中	是
电信	CNVD-2016-00789	Cisco RV220W SQL 注入漏洞	高	是
电信	CNVD-2016-00806	Westermo Industrial switches 硬编码证书漏洞	中	是
电信	CNVD-2016-00828	Cisco Small Business 500 Device Web	中	是

		GUI 拒绝服务漏洞		
电信	CNVD-2016-00845	KDDI HOME SPOT CUBE devices 跨站脚本漏洞	中	是
移动互联网	CNVD-2016-00826	Samsung KNOX 弱加密漏洞	中	是
移动互联网	CNVD-2016-00825	Samsung KNOX 信息泄露漏洞	中	是
工控系统	CNVD-2016-00720	MICROSYS PROMOTIC 堆缓冲区溢出漏洞	高	是
工控系统	CNVD-2016-00717	Rockwell Automation MicroLogix 1100 PLC 栈缓冲区溢出漏洞	高	是
工控系统	CNVD-2016-00806	Westermo Industrial switches 硬编码证书漏洞	中	是

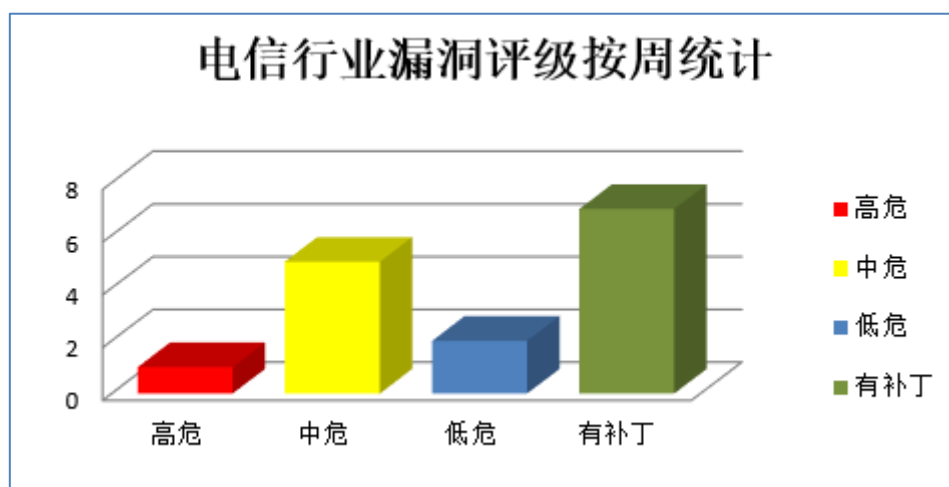


图 1 电信行业漏洞统计

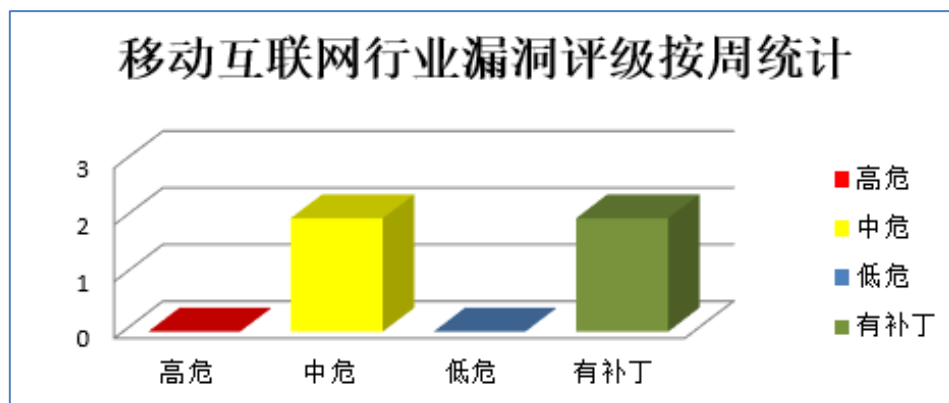


图 2 移动互联网行业漏洞统计

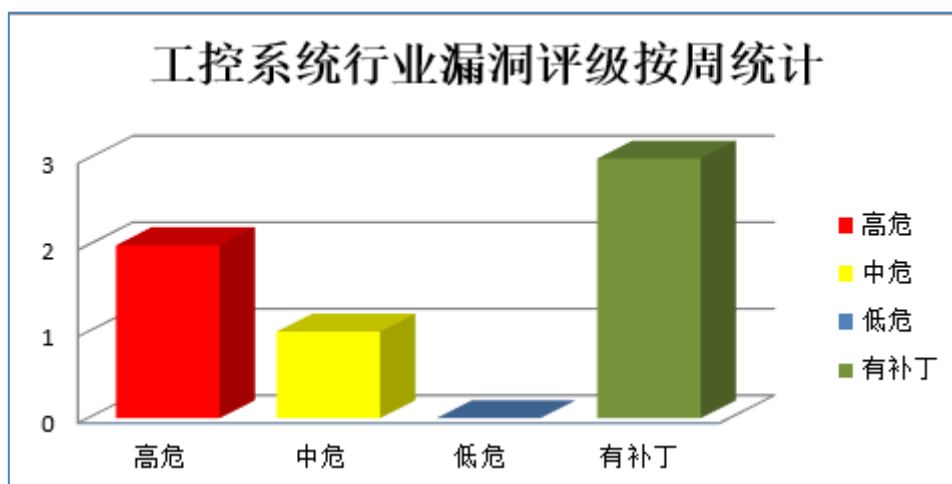


图 3 工控系统行业漏洞统计

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、OpenSSL 产品安全漏洞

OpenSSL 是一个实现安全套接层和安全传输层协议的通用开源加密库，可支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。本周，上述产品被披露存在加密算法破解、不安全算法使用漏洞。远程攻击者可利用该漏洞，获取加密密钥，并发起后续攻击，获得用户的敏感信息等。

CNVD 收录的相关漏洞包括：OpenSSL 不安全算法使用漏洞、OpenSSL 加密算法破解漏洞。其中，“OpenSSL 加密算法破解漏洞”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-2016-00805>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00711>

2、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。Google V8 是其中的一套开源 JavaScript 引擎。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可获取敏感信息、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：Google Chrome V8 拒绝服务漏洞（CNVD-2016-00780）、Google Chrome PDFium 整数溢出漏洞（CNVD-2016-00808）、Google Chrome 拒绝服务漏洞（CNVD-2016-00722）、Google Chrome Blink 信息泄露漏洞（CNVD-2016-00723）、Google Chrome Omnibox 安全绕过漏洞、Google Chrome URL 伪造漏洞、Google Chrome V8 拒绝服务漏洞（CNVD-2016-00713）、Google Chrome PDFium 内存错误引用漏洞（CNVD-2016-00714）。其中，“Google Chrome 拒绝服务漏洞（CNVD-2016-00713）”的综合评级为“高危”。

6-00722)”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-2016-00780>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00808>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00722>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00723>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00809>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00724>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00713>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00714>

3、phpMyAdmin 产品安全漏洞

phpMyAdmin 是 phpMyAdmin 团队开发的一套免费的、基于 Web 的 MySQL 数据库管理工具。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可获取敏感信息、进行跨站脚本攻击和执行未授权操作等。

CNVD 收录的相关漏洞包括：phpMyAdmin SQL 解析目录遍历漏洞、phpMyAdmin SQL 编辑跨站脚本漏洞、phpMyAdmin 密码猜测漏洞、phpMyAdmin 跨站脚本漏洞（CNVD-2016-00797）、phpMyAdmin 安全限制绕过漏洞、phpMyAdmin 目录遍历漏洞。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-2016-00799>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00800>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00798>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00797>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00796>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00795>

4、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会开发的一款开源 Web 浏览器。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可伪造地址栏、进行中间人攻击和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Mozilla Firefox 拒绝服务漏洞（CNVD-2016-00848）、Mozilla Firefox 欺骗漏洞（CNVD-2016-00849）、Mozilla Firefox 地址栏伪造漏洞（CNVD-2016-00850）、Mozilla Firefox 中间人攻击漏洞（CNVD-2016-00851）、Mozilla Firefox 拒绝服务漏洞（CNVD-2016-00847）。其中，“Mozilla Firefox 拒绝服务漏洞（CNVD-2016-00848）”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-2016-00848>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00849>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00850>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00851>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00847>

5、Cisco Unity Connection 跨站脚本漏洞 (CNVD-2016-00827)

Cisco Unity Connection 是一套语音留言平台。本周, Cisco Unity Connection 被披露存在跨站脚本漏洞, 攻击者可利用漏洞注入恶意脚本或 HTML 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-2016-00827>

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-2016-00772	Xen 'PV superpage'函数安全绕过漏洞	高	目前厂商已经发布升级补丁/版本以修复这个安全问题, 请用户及时下载更新: http://xenbits.xen.org/xsa/advisory-167.html
CNVD-2016-00778	Oracle GoldenGate 存在未明漏洞 (CNVD-2016-00778)	高	目前厂商已经发布升级补丁/版本以修复这个安全问题, 请用户及时下载更新: http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
CNVD-2016-00779	Oracle GoldenGate 组件存在未明漏洞	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.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
CNVD-2016-00786	Harman AMX 存在未明漏洞 (CNVD-2016-00786)	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.amx.com/techcenter/NXSecurityBrief/
CNVD-2016-00785	Harman AMX 存在未明漏洞	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.amx.com/techcenter/NXSecurityBrief/
CNVD-2016-00801	Lexmark 打印机竞争条件漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: http://support.lexmark.com/index?pa

			ge=content&id=TE745
CNVD-2016-00812	Cisco Wide Area Application Service CIFS 拒绝服务漏洞	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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160127-waascifs
CNVD-2016-00813	FreeBSD issetugid(2)系统调用漏洞	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.freebsd.org/security/advisories/FreeBSD-SA-16:10.linux.asc
CNVD-2016-00843	HaxxcURL 任意文件写入漏洞	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://curl.haxx.se/docs/adv_20160127B.html
CNVD-2016-00834	libEBML 内存错误引用漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://github.com/Matroska-Org/libebml/blob/release-1.3.3/ChangeLog

表 3 部分高危漏洞列表

小结：本周，OpenSSL 被披露存在加密算法破解、不安全算法使用漏洞。远程攻击者可利用该漏洞，获取加密密钥，并发起后续攻击，获得用户的敏感信息等。此外，Google、phpMyAdmin、Mozilla 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敏感信息、执行任意代码、进行跨站脚本攻击、执行未授权操作和发起拒绝服务攻击等。此外，Cisco Unity Connection 被披露存在一个跨站脚本漏洞，攻击者可利用漏洞注入恶意脚本或 HTML 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、McAfee 修补 Total Protection 产品漏洞

McAfee Total Protection 是一套杀毒软件。McAfee File Lock 是一个提供数据加密保护的文件夹锁定软件。McPvDrv.sys 是其中的一个驱动程序。

本周，McAfee 修补了上述产品存在的栈缓冲区溢出和拒绝服务漏洞，避免攻击者利用漏洞发起拒绝服务攻击。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/71188>
<http://www.cnvd.org.cn/patchInfo/show/71189>

本周要闻速递

1. 苹果 iOS 系统被曝出现漏洞: 可使锁屏密码失去作用

近日安全研究人员发现了 iOS 8 和 iOS 9 系统漏洞, 利用该漏洞可以使锁屏密码完全失去作用。目前 Benjamin Kunz Mejri 已经发布了一个 POC 演示视频。Mejri 称, 首先攻击者先执行基于访问设备次数的攻击, 绕过锁屏密码, 而恶意攻击者需要物理访问目标设备才能充分发起攻击, 恶意攻击者利用该漏洞可以欺骗目标设备获取访问权限并会进入到另外一种模式, 而接下来就会出现无限循环运行程序问题。最终锁屏密码会被停用。同时 Mejri 称, 影响的设备包括 iPhone 5、iPhone 6 手机以及 iPad 2 平板电脑。参考链接: <http://www.freebuf.com/news/95755.html>

2. 利用 AngularJS 绕过 XSS 表达式沙箱

AngularJS 是一个很流行的 JavaScript 框架, 通过这个框架可以把表达式放在花括号中嵌入到页面中。例如, 表达式 $1+2=\{\{1+2\}\}$ 将会得到 $1+2=3$ 。其中括号中的表达式被执行了, 这就意味着, 如果服务端允许用户输入的参数中带有花括号, 我们就可以用 Angular 表达式来进行 xss 攻击。

参考链接: <http://www.freebuf.com/articles/network/95497.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