

信息安全漏洞周报

2012 年 3 月 5 日-2012 年 3 月 11 日

2012 年第 10 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**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 162 个，其中高危漏洞 85 个、中危漏洞 76 个、低危漏洞 1 个。上述漏洞中，可利用来实施远程攻击的漏洞有 155 个。本周收录的漏洞中，已有 132 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。本周互联网上出现“SAP Business Objects Infoview 存在多个跨站脚本漏洞”、“Passport PC To Host '.zws'文件内存破坏漏洞”等的零日攻击代码，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 7 家成员单位报送了本周收录的全部 161 个漏洞。各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、安天实验室报送数量较多。此外，接收到成员单位安天实验室报送了一个国产办公 OA 软件系统的多处跨站漏洞（按同一类型漏洞记），目前对该漏洞通过本地测试完成验证，待协调生产厂商完成处置后择期发布。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	176	0
绿盟科技	153	0
安天实验室	32	1
东软	17	0
恒安嘉新	12	0
天融信	9	0
安氏领信	4	0
总计	162（去重）	1

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 WebKit Open Source Project、FreeType、Google、IBM 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	WebKit Open Source Project	33	20.5%
2	FreeType	19	11.8%
3	Google	16	9.9%
4	IBM	10	6.2%
5	Apple	9	5.6%
6	Mantisbt	4	2.5%
7	Etano	3	1.9%
8	phpCAS	2	1.2%
9	Joomla!	2	1.2%
10	Linux	2	1.2%
11	其它	61	38.0%

表 2 漏洞产品涉及厂商分布统计表

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、Google Chrome 安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。本周，Google Chrome 被披露存在多个安全漏洞。远程攻击者可以利用漏洞进行跨站脚本攻击，绕过安全限制，执行任意代码。CNVD 收录的相关漏洞包括：Google Chrome 存在漏洞（CNVD-2012-10381、CNVD-2012-10382、CNVD-2012-10384、CNVD-2012-10383、CNVD-2012-10371、CNVD-2012-10372、CNVD-2012-10373、CNVD-2012-10374）。上述漏洞的综合评级均为“高危”。目前，Google 已经发布这些漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42995
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42996
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42998
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42997
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42975
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42976

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42977

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42978

2、FreeType 产品安全漏洞

FreeType 是一款字体函数库。本周，FreeType 被披露存在多个综合评级为“高危”安全漏洞。远程攻击者可以利用漏洞使应用程序崩溃。CNVD 收录的相关漏洞包括：FreeType 存在漏洞（CNVD-2012-10404、CNVD-2012-10405、CNVD-2012-10406、CNVD-2012-10408、CNVD-2012-10386、CNVD-2012-10387、CNVD-2012-10388、CNVD-2012-10389）。目前，厂商已经发布这些漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43053

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43054

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43055

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43076

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43035

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43036

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43037

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43038

3、IBM 产品安全漏洞

IBM Tivoli Maximo Asset Management 软件主要用于企业资产提供管理平台。本周，上述 IBM 产品被披露存在多个安全漏洞。攻击者可以利用漏洞重定向用户请求到任意网站，发起跨站脚本或 SQL 注入攻击，窃取敏感信息或使系统崩溃。CNVD 收录的相关漏洞包括：IBM Maximo Asset Management 'uisessionid'重定向漏洞、IBM Maximo Asset Management 'controlid'跨站脚本漏洞、IBM Maximo Asset Management 'uisessionid'跨站脚本漏洞、IBM Maximo Asset Management 跨站脚本漏洞、IBM Maximo Asset Management WEB 缓存跨站脚本漏洞、IBM Maximo Asset Management SQL 注入漏洞、IBM Maximo Asset Management 跨站脚本漏洞（CNVD-2012-10438）、IBM Maximo Asset Management UI 会话存在漏洞。目前，厂商已经发布上述漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43239

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43240

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43255

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43257

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43259

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43262

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43263

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43260

4、Apple 产品安全漏洞

本周，Apple 的两款产品 Safari 和 iOS 被披露存在多个安全漏洞。Apple Safari 是一款流行的 WEB 浏览器；Apple iOS 是苹果相关终端产品操作系统。攻击者可以利用上述产品漏洞进行地址栏伪造攻击、使设备崩溃，绕过安全限制，获得敏感信息或执行任意代码。CNVD 收录的相关漏洞包括：Apple iPhone/iPad/iPod touch iOS 存在漏洞（CNVD-2012-10445、CNVD-2012-10446、CNVD-2012-10447、CNVD-2012-10448、CNVD-2012-10451、CNVD-2012-10449、CNVD-2012-10450）、Apple Safari 'setInterval()' 地址栏伪造漏洞。目前，除“Apple Safari 'setInterval()' 地址栏伪造漏洞”外，厂商已经发布其余漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43337
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43338
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43339
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43355
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43358
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43356
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43357
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43236

5、SAP Business Objects Infoview 存在多个跨站脚本漏洞

SAP Business Objects 是一款用于商务办公的产品套件，Business Objects XI 主要提供报表生成、查询和分析、绩效管理以及数据集成等功能。本周，SAP Business Objects 被披露存在多个跨站脚本漏洞。由于程序未能正确过滤用户提交的输入，攻击者可以构建恶意 URL，诱使用户解析，获得敏感信息或劫持用户会话。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 SAP Business Objects XI R2 版本。厂商尚未发布上述漏洞的修补程序，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/sites/main/preview/ldgg_preview.htm?tid=43375

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/publish/main/52/index.html>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2012-10455	Holdem Manager 存在多个内存破坏漏洞	高	暂无
CNVD-2012-10431	Exponent CMS 'src'参数 SQL 注入漏洞	高	Exponent CMS 2.0.5 已经修复此漏洞，建议用户下载使用： https://github.com/exponentcms/expone

			nt-cms/commit/f47cd477f2a96d05fbbd209f03daeb1f4d2b2eb3
CNVD-2012-10422	Joomla! SQL 注入漏洞	高	Joomla! 2.5.2 版本已修复此漏洞, 建议用户下载使用: http://developer.joomla.org/security/news/392-20120302-core-xss-vulnerability.html
CNVD-2012-10420	Timesheet Next Gen 'password' SQL 注入漏洞	高	暂无
CNVD-2012-10419	RivetTracker 'torrent_functions.php' SQL 注入漏洞	高	暂无
CNVD-2012-10416	RSA SecurID Software Token Converter 缓冲区溢出漏洞 (CNVD-2012-10416)	高	RSA Security RSA SecurID Software Token Converter 2.6.1 已经修复此漏洞, 建议用户下载使用: http://www.rsa.com/node.aspx?id=2521
CNVD-2012-10417	deVIL'z Clanportal Witze Addon 'id' SQL 注入漏洞	高	暂无
CNVD-2012-10338	AtHocGov IWSAlerts ActiveX 控件缓冲区溢出漏洞	高	暂无
CNVD-2012-10337	ContentKeeper Web 远程命令执行安全漏洞	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.contentkeeper.com/
CNVD-2012-10345	MySQL 存在未明远程代码执行漏洞 (CNVD-2012-10345)	高	暂无

表 3 部分高危漏洞列表

小结: 本周, Google Chrome 浏览器和 FreeType 产品被披露存在多个综合评级为“高危”的安全漏洞。远程攻击者可以利用漏洞进行跨站脚本攻击, 绕过安全限制, 执行任意代码, 或使系统崩溃。IBM 应用程序、Apple 浏览器和移动设备操作系统也被披露存在多个安全漏洞, 影响涉及广大终端用户。而 SAP Business Objects 零日漏洞也需引起相关用户注意, 加强防范。

CNVD 提醒使用上述软件的相关机构和个人及时采取安全防范措施。

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、Linux 发布升级程序, 修补 Kernel 安全漏洞

本周, Linux 发布升级程序, 修补了 Kernel 存在的安全漏洞。攻击者利用漏洞可导

致系统拒绝服务。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安全事件。

补丁下载链接：http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=12591
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=11991

本周要闻速递

1. Wi-Fi 联盟计划修复 Wi-Fi Protected Setup 安全漏洞

Wi-Fi 联盟已经在有关 Wi-Fi Protected Setup 方面的一份声明中对之前的安全漏洞的消息作出回应。它声称现在正对程序进行测试和认证，以确保 Wi-Fi 设备能有效抵御暴力穷举和面向 PIN 码的攻击。从最近发现的攻击中，安全人员发现黑客从开始猜解到破解 PIN 码只用不到 4 个小时。而多家厂商的 Wi-Fi Protected Setup 防护机制不到位。WPS (Wi-Fi Protected Setup, Wi-Fi 保护设置) 是由 Wi-Fi 联盟组织实施的认证项目，主要致力于简化无线局域网的安装及安全性能配置工作。在传统方式下，用户新建一个无线网络时，必须在接入点手动设置网络名 (SSID) 和安全密钥，然后在客户端验证密钥以阻止“不速之客”的闯入。这整个过程需要用户具备 Wi-Fi 设备的背景知识和修改必要配置的能力。Wi-Fi Protected Setup 能帮助用户自动设置网络名 (SSID)、配置强大的 WPA 数据编码及认证功能，用户只需输入个人信息码 (PIN 方法) 或按下按钮 (按钮设置，或称 PBC)，即能安全地连入 WLAN。这大大简化了无线安全设置的操作。Wi-Fi Protected Setup 支持多种通过 Wi-Fi 认证的 802.11 产品，包括接入点、无线适配器、Wi-Fi 电话以及其他消费性电子设备。

参考链接：<http://www.cnbeta.com/articles/175881.htm>

2. Google 在 24 小时内修复 Chrome 0day 漏洞

Google Chrome 浏览器在 Pwn2Own 黑客挑战赛开始五分钟内就被攻陷，黑客利用了 2 个 0day 漏洞。在漏洞曝光不到 24 小时后，Google 官方发布了 Chrome 17.0.963.78 更新，修复了漏洞。但在绝大多数用户完成更新前，Google 出于安全考虑没有详细披露漏洞细节，仅仅称是普遍跨站脚本攻击 (UXSS) 和有问题的历史导航。

参考链接：<http://sec.chinabyte.com/119/12286119.shtml>

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

国家互联网应急中心的全称是国家计算机网络应急技术处理协调中心（英文简称是CNCERT 或 CNCERT/CC）成立于 1999 年 9 月，是工业和信息化部领导下的国家级网络安全应急机构，致力于建设国家级的网络安全监测中心、预警中心和应急中心，以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，支持基础信息网络的安全防护和安全运行，支援重要信息系统的网络安全监测、预警和处置；国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999