

信息安全漏洞周报

2011 年 3 月 21 日-2011 年 3 月 27 日

2011 年第 12 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 102 个，其中高危漏洞 51 个、中危漏洞 26 个、低危漏洞 25 个。上述漏洞中，可利用来实施远程攻击的漏洞有 85 个。网上已经出现针对“Siemens Tecnomatix FactoryLink”、“Iconics GENESIS32/GENESIS64”等多款工控软件漏洞，以及“Real Networks RealPlayer '.ivr'文件解析堆缓冲区溢出漏洞”和“Joomla! SQL 注入漏洞”等的零日攻击代码，请使用相关产品的用户注意做好防护措施。本周收录的漏洞中，已有 70 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、多款工控软件存在安全漏洞

本周，CNVD 获知，Siemens 公司、Iconics 公司、7-Technologies 公司、RealFlex Technologies 公司和 BroadWin 公司的多款工业控制软件产品存在 36 个可以远程利用的系统漏洞（注：CNVD 成员单位安天公司及时报送了上述信息）。这些漏洞一旦被恶意利用，可造成工业控制系统主机拒绝服务，严重时还会导致工业控制系统主机被非授权控制。截至 3 月 25 日，除 BroadWin 公司的产品外，其他存在漏洞产品的攻击代码已经在互联网公开传播。由于相关厂商尚未发布安全补丁，使得上述产品的客户面临着严重的安全威胁。根据 CNVD 掌握的情况，受影响的产品均为 SCADA 系列软件，即数据采集与监视控制系统软件。这些产品广泛应用于石油、化工、电力、水利、天然气、食品加工等领域，承担着数据采集、监视控制、过程控制、信号报警、参数调节等多种任务，国内也有部分企业采用了上述存在漏洞的产品。

CNVD 提醒在工业控制系统中采用相应版本软件的用户做好防范工作，建议措施如下：

（1）最小化控制系统设备的网络暴露程度，控制系统设备不应与互联网直接相连；（2）控制系统设备及局域网应置于防火墙之后，并与办公网络隔离；（3）对控制系统设备及网络的远程访问应使用 VPN（虚拟专用网）；（4）关注操作系统厂商和控制系统厂商的安全更新，

并及时修补；（5）对控制系统设备及网络进行全面的安全审查，建立有效地安全防范措施。

参考链接：<http://www.cnvd.org.cn/notifications/145>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04779>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04769>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04767>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04750>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04794>

2、Apple Mac OS X 安全漏洞

本周，苹果公司发布了安全更新，修复了 Apple Mac OS X 存在的多个安全漏洞。攻击者可以利用这些漏洞执行任意代码、获取敏感信息或造成应用程序崩溃。CNVD 收录的漏洞包括：Apple Mac OS X 对话框使用漏洞、Apple Mac OS X 整数截断漏洞、Apple Mac OS X 跨域漏洞、Apple Mac OS X 内存破坏漏洞（CVE-2011-0186、CVE-2011-0184、CVE-2011-0179）、Apple Mac OS X 缓冲区溢出漏洞（CVE-2011-0193、CVE-2011-0177）。这些漏洞的综合评级均为“高危”。CNVD 提醒广大苹果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/vulnerability/CNVD-2011-04766>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04765>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04764>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04763>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04762>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04759>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04753>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04751>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04751>

3、PHP 产品安全漏洞

PHP 是一款流行的编程语言。本周，PHP 产品被披露存在多个拒绝服务漏洞。攻击者可以利用漏洞造成应用程序崩溃，导致拒绝服务。CNVD 收录的 PHP 漏洞包括：PHP 'Intl' 扩展 'NumberFormatter::setSymbol()' 函数拒绝服务漏洞、PHP 'Zip' 扩展 'stream_get_contents()' 函数拒绝服务漏洞、PHP 流组件远程拒绝服务漏洞、PHP 'OpenSSL' 扩展拒绝服务漏洞、PHP 'Zip' 扩展 'zip_fread()' 函数拒绝服务漏洞。互联网上已经出现了针对上述漏洞的攻击代码，影响 PHP 产品的多个版本。目前，厂商已经发布了上述漏洞的补丁程序，CNVD 提醒广大用户随时关注厂商主页以获取补丁程序或更新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04810>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04808>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04806>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04804>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04802>

4、Linux Kernel 安全漏洞

Linux Kernel 是开源操作系统 Linux 的内核。本周, Linux Kernel 出现了多个安全漏洞。攻击者可以利用漏洞提升权限、获取敏感信息或执行任意代码。CNVD 收录的具体漏洞包括: Linux Kernel SCTP 本地竞争条件漏洞、Linux Kernel 'load_mixer_volumes'函数缓冲区溢出漏洞、Linux Kernel fs/xfs/xfs_fsops.c 文件信息泄露漏洞、Linux Kernel 'ethtool.c'信息泄露漏洞、Linux Kernel 符号代码伪造本地拒绝服务漏洞、Linux Kernel 'sound/oss/midi_synth.c'内存破坏漏洞等。其中,“Linux Kernel SCTP 本地竞争条件漏洞”的综合评级为“高危”。目前, Linux 已经发布了补丁程序修复这些漏洞, CNVD 提醒广大用户及时下载更新, 避免引发漏洞相关的安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-04822>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04820>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04818>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04816>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04803>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04801>

5、Real Networks RealPlayer '.ivr'文件解析堆缓冲区溢出漏洞

RealPlayer 是一款媒体播放程序。RealNetworks RealPlayer 在解析 IVR 文件时, 帧大小由用户自主分配, 当拷贝一定数量的帧到缓冲区时可触发堆溢出。成功利用漏洞可以在受影响的程序中执行任意代码。该漏洞的综合评级为“高危”。目前, 互联网上已经出现针对该漏洞的攻击代码, 主要影响 RealNetworks RealPlayer 14.0.1/14.0.1.633/14.0.1.609/14.0.0 版本。目前, 厂商尚未发布该漏洞补丁程序, CNVD 建议用户及时关注厂商主页, 以获取补丁程序或最新版本。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-04778>

小结: 上述漏洞中, Siemens 公司、Iconics 公司、7-Technologies 公司、RealFlex Technologies 公司和 BroadWin 公司的多款工业控制软件产品存在多个可以远程利用的系统漏洞。这些漏洞一旦被恶意利用, 会危及相关的工业系统运行安全。本周, Apple 发布安全更新, 修复了 Apple Mac OS X 中存在的多个安全漏洞; 此外, PHP 产品、Linux Kernel 和 Real Networks RealPlayer 均出现了安全漏洞。上述漏洞若未能及时修补, 会对互联网网络安全及用户个人信息安全构成严重威胁, 请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

本周, CNVD 整理和发布以下重要安全修补信息。

1、Google 发布升级程序, 修补 Chrome 多个安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周, Google 发布升级程序, 修补了 Chrome 多个安全漏洞, 避免攻击者利用漏洞发起拒绝服务或任意代码执行等攻击。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安全事件。

补丁下载链接: <http://www.cnvd.org.cn/patch/3396>
<http://www.cnvd.org.cn/patch/3397>
<http://www.cnvd.org.cn/patch/3398>
<http://www.cnvd.org.cn/patch/3399>



本周要闻速递

1. Google 抢先修复 Adobe Flash 零日漏洞

北京时间 3 月 22 日消息, Google 今天修复了 Adobe Flash 的“零日漏洞”, 其补丁发布时间甚至比 Adobe 更早。据介绍, 黑客可以利用该漏洞在 Excel 文件中植入一个恶意 Flash 文件, 如果该 Excel 文件被打开, 用户电脑就有可能遭到破坏。Google Chrome 浏览器目前已经修复这一漏洞, 由于 Chrome 的 Flash 版本和更新均由 Google 控制, 因此 Google 能够在 Adobe 发布官方补丁前修复漏洞。

参考链接: http://xiazai.zol.com.cn/article_topic/221/2219160.html

2. 黑莓制造商确认安全漏洞存在

黑莓制造商 RIM 公司近日承认了黑莓手机 WebKit 浏览器存在安全漏洞, 并建议用户关闭 Web 浏览器, 以避免黑客的攻击。Pwn2Own 团队报告了这个漏洞, 主要攻击黑莓 9800。黑客可通过漏洞获悉手机联系人列表和内存卡中的照片, 但电子邮件和设备上的其他私人信息没有受到影响。RIM 回应承认该漏洞存在, 同时表示尚未收到任何黑客利用该漏洞攻击的报告。不过, 由于该漏洞已经公开, 用户不得不做出防备。值得注意的是, 黑客发起攻击, 需要诱使手机用户访问一个恶意网站, 所以当你的手机处于漫游状态时, 需要小心。另外, RIM 还给出两个建议: 个人用户可以禁用手机浏览器中的 JavaScript, 屏蔽一些网站。企业用户如果使用了黑莓企业服务器, 则公司 IT 部门可维护手机浏览器的安全。苹果 Safari 浏览器同样被曝出存在 WebKit 渲染漏洞, iPhone 4 等都是攻击目标。不过, 苹果最新的 iOS 4.3 中已经修复了该漏洞, 用户可升级, 避免受到黑客攻击。

参考链接: <http://tech.sina.com.cn/mobile/n/2011-03-18/10211687057.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