

信息安全漏洞周报

2012 年 3 月 12 日-2012 年 3 月 18 日

2012 年第 11 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 165 个，其中高危漏洞 76 个、中危漏洞 88 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 160 个。本周收录的漏洞中，已有 123 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“Presto! PageManager 存在多个安全漏洞”、“TP-LINK TL-WR740N 'ping_addr'参数 HTML 注入漏洞”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 165 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、天融信报送数量较多。此外，接收到合作单位奇虎 360 报送了某国产 CMS 建站系统存在的 3 个漏洞，此外，国内漏洞研究者（个人报送者）向 CNVD 报送了 3 起涉及政府和重要信息系统部门的漏洞事件。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	112	0
绿盟科技	168	0
天融信	62	0
安天实验室	28	0
恒安嘉新	13	0
东软	5	0
安氏领信	4	0
个人上报者	4	4

奇虎	3	3
报送总计	399	7
录入总计	165（去重）	7

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、Mozilla、Microsoft、Cisco 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	34	20.6%
2	Mozilla	12	7.3%
3	Microsoft	7	4.2%
4	Cisco	5	3%
5	HP	4	2.4%
6	Citrix	4	2.4%
7	General Electric	4	2.4%
8	TIBCO	4	2.4%
9	James Clark	3	1.8%
10	EMC	3	1.8%
11	其它	85	51.7%

表 2 漏洞产品涉及厂商分布统计表

本周涉及电信行业漏洞信息

本周，CNVD 收录了 2 个网络设备漏洞，其中“多个 Xerox 设备多个远程代码执行漏洞”的综合评级为“高危”。“TP-LINK TL-WR740N 'ping_addr'参数 HTML 注入漏洞”的综合评级为“中危”，目前，互联网上已经出现针对该漏洞的攻击代码。

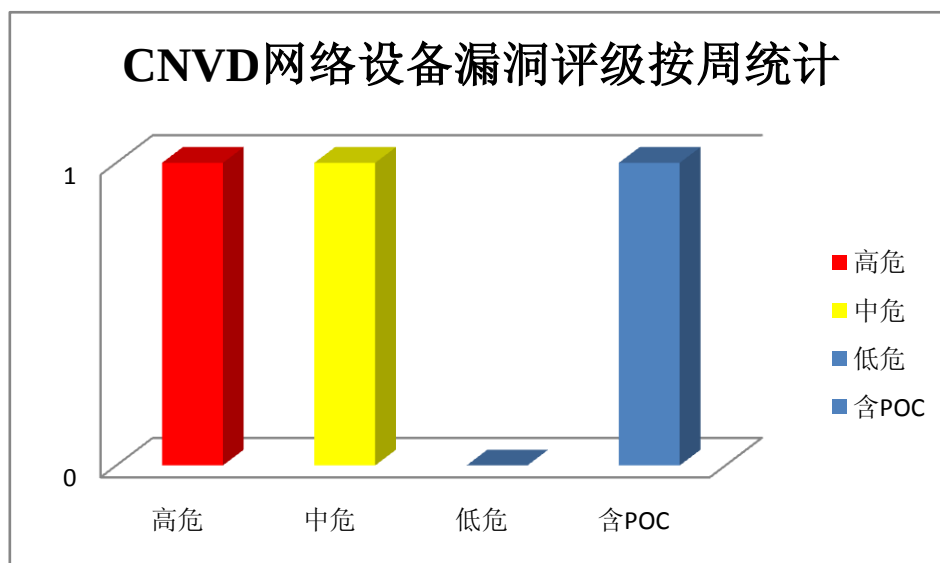


图 1 网络设备数据统计图

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、Microsoft 产品安全漏洞

3月14日，微软发布了2011年3月份的月度例行安全公告，共包含6项安全更新，修复了涉及Windows操作系统、Visual Studio开发工具和Expression Design绘图编辑工具多个产品存在的7处安全漏洞。其中MS12-020项公告的综合评级为“严重”。此项更新修复了Windows远程桌面协议中存在的两个代码执行漏洞。如果攻击者向受影响的系统发送一系列特制RDP数据包，则可导致远程执行代码。没有启用RDP的系统则不受威胁。CNVD收录的相关漏洞包括：Microsoft Windows 'DirectWrite' API 拒绝服务漏洞、Microsoft Expression 'wintab32.dll' DLL 装载任意代码执行漏洞、Microsoft 远程桌面协议远程代码执行漏洞（CNVD-2012-10596）、Microsoft 远程桌面协议拒绝服务漏洞（CNVD-2012-10597）、Microsoft Visual Studio Add-In 本地特权提升漏洞、Microsoft Windows DNS Server 远程拒绝服务漏洞（CNVD-2012-10601）、Microsoft Windows Kernel 'Win32k.sys'本地特权提升漏洞（CNVD-2012-10603）。其中，“Microsoft 远程桌面协议拒绝服务漏洞（CNVD-2012-10597）”和“Microsoft 远程桌面协议远程代码执行漏洞（CNVD-2012-10596）”的漏洞综合评级均为“高危”。CNVD提醒广大Microsoft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=43901
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43895
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43897
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43898

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43899

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43915

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43917

2、Mozilla Firefox/Thunderbird/SeaMonkey 安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。本周，上述 Mozilla 产品被披露存在多个安全漏洞，攻击者可以利用漏洞以应用程序上下文执行任意代码，构建恶意网页链接，诱使用户解析触发漏洞。CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey 'array.join'内存破坏漏洞（CNVD-2012-10627）、Mozilla Firefox/Thunderbird/SeaMonkey SVG 过滤器信息泄露漏洞（CNVD-2012-10629）、Mozilla Firefox/Thunderbird/SeaMonkey 内存破坏漏洞（CNVD-2012-10632、CNVD-2012-10633、CNVD-2012-10634）、Mozilla Firefox/Thunderbird/SeaMonkey 'cssText'内存破坏漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 内存错误引用漏洞（CNVD-2012-10630）、Mozilla Firefox/Thunderbird/SeaMonkey 'shlwapi.dll'内存错误引用漏洞。上述漏洞的综合评级均为“高危”。目前，Mozilla 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=44117

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44135

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44156

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44157

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44158

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44118

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44136

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44176

3、Cisco 产品安全漏洞

Cisco Adaptive Security Appliance 是一款思科公司提供的自适应安全设备，可提供安全和 VPN 服务的模块；Cisco AnyConnect 是一款 SSL VPN 解决方案，可通过使用 WEB 浏览器启动。本周，上述 Cisco 被披露存在多个综合评级为“高危”安全漏洞，远程未验证攻击者可以利用漏洞在系统上执行任意代码或进行拒绝服务攻击。CNVD 收录的相关漏洞包括：Cisco ASA UDP 检查引擎拒绝服务漏洞、Cisco 多个产品协议独立组播拒绝服务漏洞、Cisco Adaptive Security Appliances (ASA) 5500 Clientless VPN 远程代码执行漏洞、Cisco ASA Syslog 消息 305006 拒绝服务漏洞、Cisco ASA 威胁检测拒绝服务漏洞。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=44057

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44058

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44075

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44055

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44056

4、HP 产品安全漏洞

本周，HP 的产品 Data Protector Express 被披露存在多个未明远程代码执行漏洞。HP Data Protector Express 是一款用于中小企业的备份与恢复软件。远程攻击者利用漏洞对应用程序进行拒绝服务或执行任意代码等攻击。CNVD 收录的相关漏洞包括：HP Data Protector Express 存在未明远程代码执行漏洞（CNVD-2012-10588、CNVD-2012-10589、CNVD-2012-10590、CNVD-2012-10591）。目前，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=43855

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43858

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43857

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=43856

5、TP-LINK TL-WR740N 'ping_addr'参数 HTML 注入漏洞

TP-LINK TL-WR740N 是一款无线路由器设备。本周，上述产品被披露存在一个注入漏洞。由于传递给 maintenance/tools_test.htm 中的"ping_addr"参数的输入在返回用户之前缺少过滤，攻击者可以利用漏洞跨站脚本攻击，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 TL-WR740N 111130 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=43735

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-2012-10641	mantec Altiris WISE Package Studio 存在多个 SQL 注入漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞进行 SQL 攻击，操作数据库或控制应用程序： https://fileconnect.symantec.com/
CNVD-2012-10647	多个 Xerox 设备多个远程代码执行漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞在设备上执行任意代码： http://www.xerox.com/download/security/security-bulletin/1284332-2ddc

			5-4baa79b70ac40/cert_XRX12-003_v1.1.pdf
CNVD-2012-10624	McAfee Email/Web Security Appliance/Email Gateway 存在多个漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞获得敏感信息或绕过安全限制，进行跨站脚本和暴力破解攻击： https://kc.mcafee.com/corporate/index?page=content
CNVD-2012-10569	moviEZ HD 'avrt.dll' DLL 装载任意代码执行漏洞	高	暂无
CNVD-2012-10567	Jam Trax Xpress 'sage.dll' DLL 装载任意代码执行漏洞	高	暂无
CNVD-2012-10568	Python Web 表单哈希碰撞拒绝服务漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免造成拒绝服务攻击： http://bugs.python.org/issue13703
CNVD-2012-10566	DVD Architect 'CFHDDecoder.dll' DLL 装载任意代码执行漏洞	高	暂无
CNVD-2012-10560	Gretech GOM Player 'GomU.exe' 远程缓冲区溢出漏洞	高	暂无
CNVD-2012-10577	XnView FlashPix 插件缓冲区溢出漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免触发基于堆的缓冲区溢出： http://www.xnview.com/en/xnview.html
CNVD-2012-10612	GE Proficiency Plant Applications Suite 远程内存破坏漏洞 (CNVD-2012-10612)	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免远程攻击者可以利用此漏洞使服务崩溃或执行任意代码： http://technet.microsoft.com/en-us/security/bulletin/MS12-020

表 3 部分高危漏洞列表

小结：3 月 14 日，微软发布了 2011 年 3 月份的月度例行安全公告，共包含 6 项安全更新，修复了涉及 Windows 操作系统、Visual Studio 开发工具和 Expression Design 绘图编辑工具多个产品存在的 7 处安全漏洞。其中 MS12-020 项公告的综合评级为“严重”。此项更新修复了 Windows 远程桌面协议中存在的两个代码执行漏洞。

本周，Mozilla 和 Cisco 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以应用程序上下文执行任意代码。HP 产品被披露存在多个未明

远程代码执行漏洞，攻击者可以利用漏洞对应用程序进行拒绝服务或执行任意代码等攻击。而 TP-LINK TL-WR740N 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、Citrix 发布升级程序，修补 Licensing 安全漏洞

本周，Citrix 发布升级程序，修补了 Licensing 存在的安全漏洞。避免攻击者利用漏洞构建恶意 URI，诱使用户解析，获得敏感信息或劫持用户会话，以目标用户上下文执行管理操作，访问 WEB 应用程序的攻击阻止其他合法用户访问系统。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=13511

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=13491

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=13492

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=13313

本周要闻速递

1. 微软最新安全漏洞遭泄露

北京时间 3 月 17 日消息，据路透社报道，由于中国一家黑客网站公布了微软一个安全漏洞的攻击方式，使得微软的安全漏洞分享信息流程遭到猛烈抨击。微软一般会提前向 70 多家安全公司透露新发现的重大漏洞，此次被称为“概念验证”（proof-of-concept）的代码漏洞可能就是由其中一家安全公司泄露的。微软表示，它正在对此展开调查，并“将采取必要行动保护消费者，并确保分享的机密信息按照合同和项目的要求进行保护”。微软的可信赖计算工作主管 Yunsun Wee 表示，“概念验证”代码的细节与微软向主动防御项目合作伙伴透露的漏洞信息吻合。微软于 2008 年启动主动防御项目，提前告知各安全公司将要发布的补丁，一般是提前一天。这个项目旨在使补丁全面安装到客户的电脑中之前，使得这些安全公司有时间优先研究和测试这些补丁。信息安全公司 Sophos 安全顾问格拉汉姆·克鲁利（Graham Cluley）在公司博客上表示，在发现蠕虫病毒出现更恶意目的之前，Windows 用户应当高度注意，并加强防御，尽快为自己的电脑打上补丁。

参考链接：<http://scitech.people.com.cn/h/2012/0317/c227887-4144572239.html>

2. Adobe Flash Player 更新修补两个漏洞

Adobe Systems 有限公司已经发布一个关键的 Adobe Flash Player 更新补丁，并且在它的建议中公布新的组成内容，即添加了优先级评分机制以便补丁管理员们能够估计更新补丁的严重性。该软件巨人修补了 Flash Player 的两个漏洞，这两个漏洞可以被攻击者用来执行恶意代码或是造成拒绝服务的状况。Adobe 公司表明这些错误之一可能被攻击者通过未详细说明的途径来获得敏感信息。周一发布的更新补丁影响在 Windows、Macintosh、Linux 和 Solaris 平台，以及在 Google 的安卓设备上运行 Flash Player 软件的用户。该 Flash Player 更新补丁是第一个使用 Adobe 公司的优先级评分系统的。本周发布的该关键更新补丁被给予“优先级 2”的评分，意味着当前还没有已知的 exploits 被广泛传播，并且 Adobe 公司预期没有任何瞄准该缺陷的 exploits 将要出现。上个月 Adobe 公司在 Mozilla 公司的 Firefox 浏览器中引入对它的 Flash Player 保护模式的支持功能。该公司一直在为浏览器组件设计一个沙箱环境。该保护模式在 Google 公司的 Chrome 浏览器也可使用，将 Flash Player 与关键的进程进行隔离，这使得攻击者突破 Flash 组件进入受害者的系统更为困难。

参考链接：<http://sec.chinabyte.com/92/12292092.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