

信息安全漏洞周报

2011 年 2 月 21 日-2011 年 2 月 27 日

2011 年第 8 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 102 个，其中高危漏洞 27 个、中危漏洞 26 个、低危漏洞 49 个。上述漏洞中，可被利用于实施远程攻击的漏洞有 88 个；目前，网上已经出现了“Winmerge ‘winmerge’ 项目文件缓冲区溢出”、“VicFTPS ‘LIST’ 命令远程拒绝服务”等漏洞的零日攻击代码，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 75 个漏洞具备官方修补方案，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 整理和发布了以下重要安全漏洞信息。

1、ISC BIND 9 IXFR Transfer/DDNS 更新远程拒绝服务漏洞

本周，ISC 发布公告称该公司开发的主流域名解析服务软件——BIND 9 存在高危漏洞，该漏洞可被利用于发起远程拒绝服务攻击。CNVD 认为该漏洞对国内采用相应版本软件的域名解析服务器构成严重的安全威胁，综合评级为“高危”。经分析，BIND 9.7.1、9.7.2 在处理 IXFR（Incremental zone transfer，增量区域传输）时会在一个小的时间窗口内将其区域内存数据库（in-memory zone database）锁定，如果在该时间窗口服务器再收到查询请求，则会引起死锁，导致无法响应正常的请求产生拒绝服务。向 BIND 服务器发起的查询请求速率和更新频率越高，则发生拒绝服务的可能性越大。目前，ISC 尚未发布官方补丁。CNVD 提醒使用相应版本软件的用户做好防范工作，建议措施如下：（1）目前已知受漏洞影响的 BIND 软件版本有 9.7.1-P3 和 9.7.2-P3，而 9.8、9.7.3 和 9.6.X 及以下版本不受影响，建议使用受漏洞影响 BIND 版本的用户做好软件更新及相关应用部署工作；（2）对于使用 BIND 版本为 9.7.2 的用户，如果暂时无法进行软件更新，可临时在系统启动时使用参数“-n 1”，即强制域名服务器使用单线程处理所有数据，避开带有攻击意图的域名请求。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04293>

2、Oracle 产品安全漏洞

Java SE 是用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 平台环境。本周，Oracle 公司的产品 Java SE 和 Java for Business 存在多个综合评级为“高危”的未明漏洞。CNVD 收录的漏洞包括：Oracle Java SE 和 Java for Business 多个未明漏洞（CV

E-2010-4452, CVE-2010-4454, CVE-2010-4462, CVE-2010-4463, CVE-2010-4465, CVE-2010-4467, CVE-2010-4469, CVE-2010-4473)。远程攻击者可利用未知向量影响完整性、机密性和可用性。目前,厂商已经提供了这些漏洞的补丁信息,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-2011-04288>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04287>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04286>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04285>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04284>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04283>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04282>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04281>

3、Linux Kernel 安全漏洞

Linux Kernel 是开源操作系统 Linux 所使用的内核。本周, Linux Kernel 被披露存在多个安全漏洞。CNVD 收录的漏洞包括: Linux Kernel ATI Radeon R300 本地输入验证漏洞、Linux Kernel 'drivers/infiniband/core/uverbs_cmd.c'文件整数溢出漏洞、Linux Kernel 'net/bridge/br_multicast.c'文件拒绝服务漏洞、Linux Kernel 'fs/partitions/ldm.c'拒绝服务漏洞、Linux Kernel 'fs/partitions/ldm.c'缓冲区溢出漏洞、Linux Kernel 'procfs'和'sysfs'本地安全绕过漏洞、Linux Kernel 'ib_uverbs_poll_cq()'函数本地信息泄漏漏洞。其中,“Linux Kernel ATI Radeon R300 本地输入验证漏洞”的综合评级为“高危”。目前, Linux 已经发布了这些漏洞的补丁程序, CNVD 提醒广大用户及时下载更新,避免引发此类漏洞相关的安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-04364>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04343>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04341>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04339>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04338>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04298>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04294>

4、皮皮播放器安全漏洞

PIPI Player (皮皮播放器)是一款国内流行的高清电视播放器。本周, CNVD 收录 PIPI Player 两个综合评级为“高危”的安全漏洞,包括:皮皮播放器 ActiveX 控件 PlayURLWithLocalPlayer()函数溢出漏洞和皮皮播放器 ActiveX 控件 PlayURL()函数溢出漏洞。该漏洞是由于 PIPI Player 的 ActiveX 控件 (PIPIWebPlayer.ocx) 中的 PlayURLWithLocalPlayer()函数和 PlayURL()函数在处理 URL 地址时没有进行有效的参数过滤,存在栈溢出漏洞。远程攻击者可以利用漏洞在受影响的程序中执行任意代码。目前,厂商尚未发布这两个漏洞

的补丁程序，CNVD 提醒广大用户随时关注厂商主页，并加强防范措施。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-04301>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04300>

5、WinMerge '.winmerge'项目文件缓冲区溢出漏洞

WinMerge 是一款运行于 Windows 系统下免费开源的文件比较/合并工具。WinMerge 在解析.winmerge 项目文件时并没有严格检查用户的文件格式，可以利用栈缓冲区溢出发起攻击。攻击者通过构建特制文件，诱使用户解析，进而可执行任意代码。目前，互联网上已经出现了针对该漏洞的攻击代码，主要影响版本为 WinMerge 2.12.4.0 Unicode。目前，厂商尚未发布此漏洞的补丁程序，CNVD 提醒广大用户随时关注厂商主页以获取最新版本，避免引发漏洞相关的安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-04308>

小结：本周，ISC 公开了 BIND 9 存在的高危漏洞，该漏洞可被利用于发起远程拒绝服务攻击。CNVD 在漏洞公布之前获知了相关情况，并对漏洞进行了跟踪分析。鉴于该漏洞可能对国内众多采用相应软件的域名服务器构成严重威胁，对其风险综合评级为“高危”，相关用户可采用 ISC 提供的临时解决方案或对软件进行升级加以应对。Oracle 的产品 Java SE 和 Java for Business 存在多个“高危”的未明漏洞。此外，Linux Kernel、PIPI Player 和 Winmerge 均出现了安全漏洞，对互联网用户的信息安全和网络安全构成较为严重的威胁，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、Cisco 发布升级程序，修补了 TelePresence 多个安全漏洞

Cisco TelePresence 是思科公司开发的网络会议解决方案。本周，Cisco 发布多个升级程序用于修补了 TelePresence 产品的多个安全漏洞，避免攻击者可以利用漏洞提升特权、获得敏感信息、进行拒绝服务和任意代码执行攻击。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/3052>
<http://www.cnvd.org.cn/patch/3053>
<http://www.cnvd.org.cn/patch/3054>
<http://www.cnvd.org.cn/patch/3088>

本周要闻速递

1. Ixia 近日发布了网络漏洞测试工具 IxLoad-Attack

2 月 23 日消息，Ixia 作为融合 IP 网络测试解决方案提供商，于近日发布了网络漏洞测试

试工具 IxLoad-Attack。Ixia 在 2 月 14 到 17 日在旧金山举办的 2011 年 RSA 大会上进行首次公开演示。IxLoad-Attack 借助业界最全面的数据库(其中包含 6,000 多个独一无二的攻击), 在一个可控的环境中, 可以利用已发布的漏洞重新构造恶意流量, 并且生成达到互联网规模的分布式拒绝服务(DDoS)攻击。

参考链接: <http://www.rfidchina.org/news/readinfos-51693-396.html>

2. 微软修复一系列反病毒软件中的共同漏洞

2 月 25 日消息, 微软修复了其防病毒和反间谍软件的漏洞, 这些漏洞可以让攻击者在本地系统上获取 LocalSystem 权限, 进行权限提升。由于反恶意软件程序的更新大多会自动完成, 因此大多数最终用户和管理员将不需要做任何事情, 该更新将在 48 个小时内分发完毕。该漏洞被评级为“重要”。涉及 Windows Live OneCare, Microsoft Security Essentials, Windows Defender, Microsoft Malicious Software Removal tool, Forefront Client Security 和 Forefront Endpoint Protection 2010 等软件。

参考链接: <http://www.hackbase.com/news/2011-02-25/41146.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