

信息安全漏洞周报

2012 年 1 月 16 日-2012 年 1 月 29 日

2012 年 第 3、4 期合刊

本周漏洞基本情况

1 月 16 日至 1 月 29 日期间信息安全漏洞威胁整体评价级别为中。

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 117 个，其中高危漏洞 28 个、中危漏洞 73 个、低危漏洞 16 个。上述漏洞中，可利用来实施远程攻击的漏洞有 103 个。本周收录的漏洞中，已有 89 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“Eudora World Mail imapd 'LIST'命令缓冲区溢出漏洞”、“Cloupia FlexPod Management 和 Automation 目录遍历漏洞”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 5 个成员单位和 1 个合作伙伴向 CNVD 报送了 1 月 16 日至 1 月 29 日收录的全部 117 个漏洞。各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰报送数量较多。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	275	0
启明星辰	213	0
安天实验室	57	0
恒安嘉新	16	0
天融信	8	0
安氏领信	4	0
总计	117（去重）	0

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、IBM、Apache 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	Oracle	47	40.2%
2	IBM	8	6.8%
3	Apache	5	4.3%
4	Moodle	3	2.6%
5	Cisco	2	1.7%
6	Rockwall Automation	2	1.7%
7	XnView	2	1.7%
8	SonicWALL	2	1.7%
9	Microsoft	1	0.9%
10	Adobe	1	0.9%
11	其它	44	37.5%

表 2 漏洞产品涉及厂商分布统计表

本周重要漏洞信息

1 月 16 日至 1 月 29 日，CNVD 整理和发布以下重要安全漏洞信息。

1、Oracle 产品安全漏洞

1 月 18 日，Oracle 公司发布了 2012 年 1 月的安全更新，修复了其多款产品存在的 78 个安全漏洞，主要包括了 27 个 MySQL Product Suite 的漏洞，17 个 Sun Products Suite 的漏洞，11 个 Oracle Fusion Middleware 漏洞，以及 Database（2 个）、E-Business Suite（3 个）、Oracle Supply Chain（1 个）、PeopleSoft（6 个）和 Oracle Virtualization Product Suite（3 个）等多个影响产品的漏洞。其中仅有一个涉及 Solaris 操作系统的漏洞（CVE-2012-0094）综合评级为“高危”。61 个安全漏洞可被远程利用。利用上述漏洞，远程或本地攻击者可以进行拒绝服务、SQL 注入和跨站脚本等攻击，进而获得敏感信息，操作数据库，执行任意代码或提升特权。CNVD 收录的相关漏洞包括：Oracle MySQL Server 存在未明漏洞（CNVD-2012-09538、CNVD-2012-09537）、Oracle Glass Fish Enterprise Server 敏感信息泄露漏洞（CNVD-2012-09484）、Oracle Solaris 存在漏洞（CNVD-2012-09493）、Oracle OpenSSO 管理组件数据操作漏洞、Oracle E-Business Suite 数据操作漏洞（CNVD-2012-09511）、Oracle Database 存在漏洞（CNVD-2012-09509）、Oracle Application Server 跨站脚本漏洞（CNVD-2012-09504）。CNVD 提醒 Oracle 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=37833
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37832
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37728

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37753

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37770

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37781

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37779

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37774

2、IBM 产品安全漏洞

本周，IBM 产品 WebSphere Application Server 被披露存在多个安全漏洞。IBM WebSphere Application Server(WAS)是由 IBM 遵照开放标准，如 Java EE、XML 和 Web Services 开发并发行的一种 Web 应用服务器。利用上述产品漏洞，攻击者可以进行跨站脚本或拒绝服务等攻击，获取敏感信息、劫持用户会话、修改文件或执行任意代码。CNVD 收录的相关漏洞包括：IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2012-09490）、IBM WebSphere Application Server 哈希碰撞拒绝服务漏洞、IBM WebSphere Application Server 'iscdeploy'脚本不安全文件权限漏洞、IBM WebSphere Application Server z/OS 跨站脚本漏洞、IBM WebSphere Application Server z/OS 存在未明漏洞。目前，IBM 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=37750

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37679

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37448

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37252

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37253

3、Cisco 产品安全漏洞

本周，Cisco 产品 IP Video Phone E20 TE 和 Digital Media Manager 存在两个综合评级为“高危”的漏洞。Cisco IP Video Phone E20 TE 是一款 IP 视频电话系统软件；Cisco Digital Media Manager 是一款数字媒体管理软件。利用上述漏洞，远程攻击者可以提升权限或绕过验证。CNVD 收录的相关漏洞包括：Cisco IP Video Phone E20 默认 ROOT 凭据验证绕过漏洞、Cisco Digital Media Manager 远程特权提升漏洞（CNVD-2012-09483）。目前，Cisco 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=37711

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37714

4、Apache 产品安全漏洞

本周，Apache 多款产品 Tomcat、HTTP Server、Struts 被披露存在多个安全漏洞。Apache Tomcat 是一款开源的基于 JSP 的 WEB 服务软件；Apache HTTP Server 是一款开源的 WEB 服务软件；Apache Struts 是一款建立 Java web 应用程序的开源运行环境软

件。攻击者可以利用上述产品漏洞执行任意代码、发起拒绝服务攻击或绕过安全限制。CNVD 收录的相关漏洞包括：Apache Tomcat 的 HTTP 摘要认证存在漏洞、Apache Tomcat 参数处理拒绝服务漏洞、Apache Tomcat 信息泄露漏洞、Apache HTTP Server Scoreboard 本地安全绕过漏洞、Apache Struts 远程命令执行漏洞（CNVD-2012-09436）。其中，“Apache Tomcat 参数处理拒绝服务漏洞”和“Apache Struts 远程命令执行漏洞（CNVD-2012-09436）”的综合评级为“高危”。目前，厂商已经发布上述漏洞的补丁程序。CNVD 提醒广大用户随时关注厂商主页，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=37772
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37649
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37650
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37248
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37309

5、Eudora WorldMail imapd 'LIST'命令缓冲区溢出漏洞

Eudora WorldMail 是一款邮件管理服务软件。本周，Eudora WorldMail 被披露存在一个缓冲区溢出漏洞。由于 Eudora WorldMail imapd 未能正确处理'LIST'命令，远程攻击者可以利用漏洞提交恶意请求触发缓冲区溢出，成功利用漏洞可以以应用程序上下文执行任意代码。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 WorldMail 3.0 版本。厂商尚未发布该漏洞的修补程序，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=37251

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-2012-09514	PhpBridges 博客系统 members.php SQL 注入漏洞	高	目前官方已对此漏洞发布相关补丁和处理方案，请及时更新软件到最新版本或安装相应补丁： https://launchpad.net/phpbridges
CNVD-2012-09513	pGB kommentar.php SQL 注入漏洞	高	目前官方已对此漏洞发布相关补丁和处理方案，请及时更新软件到最新版本或安装相应补丁： http://www.powie.de/
CNVD-2012-09482	Sysax Multi Server 'Content-Disposition'缓冲区溢出漏洞	高	Codeorigin Sysax Multi Server 5.52 已经修复此漏洞，建议用户下载使用： http://www.sysax.com/
CNVD-2012-09488	WHMCompleteSolution 'functions.php'任意代码执行漏洞	高	暂无
CNVD-2012-09478	XnView PSD 记录类型解析整数溢出漏洞（CNVD-2012-09478）	高	XnView 1.98.5 已经修复此漏洞，建议用户下载使用：

			http://www.xnview.com/
CNVD-2012-09477	Adobe Acrobat/Reader 远程整数溢出漏洞 (CNVD-2012-09477)	高	用户可参考如下供应商提供的安全公告获得补丁信息: http://www.adobe.com/support/security/bulletins/apsb11-24.html
CNVD-2012-09507	deV!L`z Clanportal SQL 注入漏洞	高	目前官方已对此漏洞发布相关补丁和处理方案, 请及时更新软件到最新版本或安装相应补丁: http://www.dzcp.de/downloads/
CNVD-2012-09505	Blade API Monitor 的 Unicode 堆栈缓冲区溢出漏洞	高	暂无
CNVD-2012-09474	BS.Player 缓冲区溢出漏洞	高	暂无
CNVD-2012-09473	Joomla! Discussions 组件'catid' SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结: 1月18日, Oracle 公司发布了 2012 年 1 月的安全更新, 修复了其多款产品存在的 78 个安全漏洞, 涉及应用广泛的轻型数据库系统 Mysql 以及其他 Oracle 应用软件中间件。远程或本地攻击者可以进行拒绝服务、SQL 注入和跨站脚本等攻击, 进而获得敏感信息以及数据库管理权限, 甚至可以执行任意代码或取得系统权限。同时, IBM、Cisco 和 Apache 的产品也被披露存在多个安全漏洞, 特别是 Apache Tomcat、HTTP Server、Struts 等广泛应用于搭建 Web 信息系统的服务软件存在的高危漏洞, 导致政府、企业以及个人网站受到直接威胁。

此外, Adobe 也在其官网发布安全更新, 修复 Acrobat/Reader 多个安全漏洞。Joomla! 和 PhpBridges 等多个 WEB 应用产品存在的“高危”漏洞和 Eudora WorldMail 零日漏洞也对用户构成安全威胁。

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、Adobe 发布升级程序, 修补 Adobe Acrobat/Reader 安全漏洞

本周, Adobe 发布升级程序, 修补 Adobe Reader/Acrobat 存在的安全漏洞。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。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/ldgg_preview.htm?tid=37708

本周要闻速递

1. 甲骨文发布安全补丁 修复多个漏洞

据国外媒体报道,甲骨文网站发布声明称,甲骨文发布 78 个安全补丁,修复其数据库、中间件软件和应用程序中的安全漏洞。甲骨文称,有 27 个补丁是修复 MySQL 数据库中的安全漏洞。其中一个安全漏洞不需要登录证书就可以在网络上利用。按照通用安全漏洞评分系统(CVSS)数据库的评分,MySQL 数据库安全漏洞的最高等级是 5.5,属于中等风险等级。另外两个补丁修复甲骨文数据库中的安全漏洞。甲骨文为 Fusion 中间件软件发布 11 个补丁。其中修复的 5 个安全漏洞能够远程利用,不需要用户身份识别。在应用程序方面,甲骨文电子商务套装软件得到 3 个安全补丁。供应链应用套装软件得到 1 个安全补丁。JD Edwards 软件得到 8 个补丁。大约 17 个安全补丁与 Sun 的产品有关,其中包括 6 个不需要证书就可以远程利用的安全漏洞。受影响的产品包括 GlassFish 企业服务器和 Solaris OS。另外 3 个补丁用于甲骨文包括 VirtualBox 在内的虚拟化技术。

参考链接: <http://sec.chinabyte.com/12/12245512.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