

信息安全漏洞周报

2011 年 8 月 22 日-2011 年 8 月 28 日

2011年第34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**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 102 个，其中高危漏洞 56 个、中危漏洞 43 个、低危漏洞 3 个。上述漏洞中，可利用来实施远程攻击的漏洞有 99 个。网上已经出现针对“Apache HTTP Server 远程拒绝服务漏洞”、“Freefloat FTP Server 'ALLO'命令远程缓冲区溢出漏洞”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 73 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。

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 102 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、恒安嘉新报送的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
绿盟科技	77	0
恒安嘉新	50	0
启明星辰	48	0
东软	5	0
安天	3	0
知道创宇	2	0
安氏领信	1	0
总计	102（去重）	0

表 1 成员单位上报漏洞统计表

本周，CNVD 整理和发布的漏洞涉及 WordPress、Google、Cisco、Apache、Linux 等多家厂商的产品，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	WordPress	11	10.8%
2	Google	11	10.8%
3	KIWI Image System	11	10.8%
4	Cisco	8	7.8%
5	GPL Host	8	7.8%
6	Pidgin	3	2.9%
7	Linux	3	2.9%
8	PHP	2	2.0%
9	Apache	2	2.0%
10	Aspcms	2	2.0%
11	其它	41	40.2%

表 2 漏洞产品涉及厂商分类统计

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、Apache HTTP Server 远程拒绝服务漏洞

本周，CNVD 多家成员单位报送了 Apache HTTP Server 存在的一个远程拒绝服务漏洞。根据 CNVD 分析结果，Apache HTTP Server 在处理 HTTP 请求包中 Range 选项时存在不安全策略(Range 头选项定义了页面文件的分片请求方式)。攻击者通过设置较大的 Range 头选项阈值以构造尽可能多的、请求不同大小页面文件的指令，可以达到消耗服务器内存和 CPU 资源的目的。攻击者还可以通过加载 “Accept-Encoding” 选项进一步增强攻击的效果。轻则导致 Apache 无法响应正常的用户请求，严重的还会导致服务器系统资源耗尽。由于 Apache HTTP Server 应用极其广泛，漏洞利用方法简单，且互联网上已经出现了攻击代码，各单位需注意加强安全防范措施。CNVD 对该漏洞的技术评级为“中危”。但由于该漏洞影响涉及 Apache HTTP Server 已知所有版本，对相关用户的网站信息系统构成较为严重的威胁。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-06943>

2、E3 CMS 安全漏洞

本周，CNVD 在官网发布了颖源 E3 CMS 内容管理软件存在的多个安全漏洞。7 月 25 日，CNVD 接到中国电力科学研究院信息安全实验室上报的颖源 E3 CMS 2006 软件的多个安全漏洞，部分漏洞可被利用获得系统管理员权限。CNVD 收录的漏洞包括：E3 CMS 任意文件上传漏洞、E3 CMS 敏感信息泄露漏洞、E3 CMS 越权访问漏洞。其中，“E3 CMS 任意文件上传漏洞、E3 CMS 越权访问漏洞”的综合评级为“高危”。目前，

厂商尚未发布这些漏洞的修补程序，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/vulnerability/CNVD-2011-06454>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06453>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06452>

3、Google Chrome 安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，Google 发布安全更新，修复 Chrome 存在的多个安全漏洞。攻击者可以利用漏洞绕过安全限制，执行任意代码或使应用程序崩溃。CNVD 收录的相关漏洞包括：Google Chrome 'memset()'和 PDF 存在漏洞（CVE-2011-2839）、Google Chrome 整数溢出漏洞（CVE-2011-2829）、Google Chrome 越界写漏洞（CVE-2011-2828）、Google Chrome 内存错误引用漏洞（CVE-2011-2827、CVE-2011-2825、CVE-2011-2824、CVE-2011-2823）、Google Chrome 绕过跨域策略漏洞（CVE-2011-2826）等。上述漏洞的综合评级均为“高危”。CNVD 提醒广大 Google 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-2011-06997>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06938>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06937>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06935>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06933>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06926>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06924>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06934>

4、Domain Technologie Control 安全漏洞

Domain Technologie Control 是一款用在商业主机的控制面板。本周，Domain Technologie Control 被披露存在多个安全漏洞。攻击者可以利用漏洞提升特权、注入任意代码、通过目录遍历攻击包含本地任意文件、获得敏感信息或劫持用户会话。CNVD 收录的漏洞包括：Domain Technologie Control 特权提升漏洞、Domain Technologie Control 'vps_node'参数 SQL 注入漏洞、Domain Technologie Control 目录遍历漏洞、Domain Technologie Control 敏感信息泄露漏洞、Domain Technologie Control 密码获取漏洞、Domain Technologie Control SQL 注入漏洞、Domain Technologie Control MySQL 用户密码泄露漏洞、Domain Technologie Control 注入漏洞。上述漏洞中，“Domain Technologie Control 特权提升漏洞”、“Domain Technologie Control 'vps_node'参数 SQL 注入漏洞”、“Domain Technologie Control SQL 注入漏洞”和“Domain Technologie Control 注入漏洞”的综合评级均为“高危”。目前，厂商已经发布上述漏洞的补丁程序，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/vulnerability/CNVD-2011-06915>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06913>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06912>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06910>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06909>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06908>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06907>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06905>

5、WordPress 插件安全漏洞

WordPress 是一款使用 PHP 语言开发的内容管理系统。本周, WordPress 多款插件被披露存在多个安全漏洞, 攻击者可以利用漏洞注入任意代码, 获得敏感信息。CNVD 收录的漏洞包括: WordPress 插件 SendIt SQL 注入漏洞、WordPress Yoast 本地文件泄露漏洞、WordPress 插件 Redirection 'id'参数跨站脚本漏洞、WordPress UnGallery 'source_vuln.php'本地文件泄露漏洞、WordPress UnGallery 'zip'参数本地文件泄露漏洞、WordPress 插件'index.php' SQL 注入漏洞、WordPress 插件 MM Duplicate SQL 注入漏洞、WordPress 插件 WP Symposium 'uid' SQL 注入漏洞。上述漏洞中, “WordPress 插件 SendIt SQL 注入漏洞、WordPress 插件'index.php' SQL 注入漏洞、WordPress 插件 MM Duplicate SQL 注入漏洞、WordPress 插件 WP Symposium 'uid' SQL 注入漏洞”的综合评级为“高危”。目前, 除 “WordPress Yoast 本地文件泄露漏洞、WordPress UnGallery 'source_vuln.php'本地文件泄露漏洞、WordPress 插件'index.php' SQL 注入漏洞”外, 厂商已经发布其余漏洞的补丁程序, CNVD 提醒广大 WordPress 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-2011-06987>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06982>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06975>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06967>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06964>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06959>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06927>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06919>

6、Cisco 产品安全漏洞

本周, Cisco 发布安全更新, 修复 Cisco 存在的多个安全漏洞。攻击者可以利用漏洞获得敏感信息, 或使服务程序崩溃、重载。CNVD 收录的相关漏洞包括: Cisco Unified Communications Manager/Presence Server 信息泄露漏洞、Cisco Unified Communications Manager (CUCM)拒绝服务漏洞 (CVE-2011-2564、CVE-2011-2563、CVE-2011-2562、

CVE-2011-2561、CVE-2011-2560)、Cisco IOS SSH2 会话远程拒绝服务漏洞 (CVE-2011-1624)、Cisco IOS 数据链路交换远程拒绝服务漏洞 (CVE-2011-1625)。上述漏洞中,除“Cisco IOS 数据链路交换远程拒绝服务漏洞 (CVE-2011-1625)”外,其余漏洞综合评级均为“高危”。CNVD 提醒广大 Cisco 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-2011-06952>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06951>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06950>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06949>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06948>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06947>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06925>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06921>

小结: 本周, Web 服务器程序以及应用组件安全较为突出, 其中, Apache HTTP Server 存在的漏洞为 0day 漏洞, 有可能引起互联网上的大规模网络攻击事件, 而开源 E3 CMS 和 Wordpress 等网站内容管理系统的多个高危漏洞也会导致网站信息系统被黑客控制。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、Linux 发布升级程序, 修补 Kernel 安全漏洞

Linux 是一款开源的操作系统。本周, Linux 发布升级程序, 修补了 Kernel 存在的安全漏洞。攻击者可以利用漏洞引起应用程序崩溃或产生其他未明影响。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/4833>

本周要闻速递

1. 谷歌更新修复 Chrome 浏览器漏洞

据国外媒体报道, 谷歌发布了 Chrome 网络浏览器的更新版本, 修复了 11 个安全漏洞。其中包括一个最严重的错误, 即存储器崩溃的缺陷, 在其余 10 个漏洞中, 9 个级别为“非常重要”, 1 个为“中等重要”。另外, 此次更新还修复了四个被描述为“user-after-free”的漏洞, 即攻击者利用恶意编码注入到用户的计算机, 从而使攻击者访问受害人

的系统。为了找出 Chrome 浏览器的缺陷，谷歌为外界的研究人员推出了错误赏金狩猎计划。按照该计划，这次谷歌总共支付了 8837 美元。目前，用户可以从谷歌官网下载最新版本的 Chrome 浏览器。

参考链接: http://news.xinhuanet.com/it/2011-08/24/c_121905085.htm

2. 微软测试 38 家软件厂商产品，暗揭苹果/谷歌产品漏洞

微软从去年 7 月份开始，其漏洞安全研究小组（MSVR）就开始对来自 38 家软件厂商的 109 款热门软件进行测试，了解它们存在的安全漏洞情况，其中就包括苹果和谷歌。微软成立该部门的宗旨是对 Windows 系统中经常运行的应用程序进行分析，掌握它们对系统安全性的影响。经调查发现，苹果 Safari 浏览器和谷歌 Picasa 等产品存在安全漏洞。Safari 支持的某种网页内容运行方式存在异常，黑客可利用该漏洞远程执行恶意脚本代码，从而获取用户重要的隐私数据。另有 WordPress 也存在类似漏洞。整个研究小组成立以来，已经列举了 93 个被标识为“重要”和“紧急”的安全漏洞。97%的厂商对漏洞采取修复措施，29%的漏洞已经彻底修复完善。前些时候，谷歌曾经针对 IE 推出一款 ChromeFrame 插件，该插件旨在使用 Chrome 引擎来帮助 IE 浏览器提高加载速度。但微软随即回应称，ChromeFrame 插件会导致系统严重的安全隐患，建议用户不要安装。

参考链接: <http://news.newhua.com/news/2011/0827/130903.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

