

信息安全漏洞周报

2010 年 8 月 9 日-2010 年 8 月 15 日

2010年第31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 90 个，其中高危漏洞 14 个、中危漏洞 22 个、低危漏洞 54 个。上述漏洞中，可利用来实施远程攻击的漏洞有 72 个。经检测发现，网上已经出现针对“Lynx 浏览器‘convert_to_idna ()’函数远程堆缓冲区溢出漏洞”的零日攻击代码，请相关用户注意做好相关防护措施。目前，有关厂商已针对 61 个漏洞提出了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。

本周重要的漏洞信息

本周，CNVD 整理和发布以下重要漏洞信息。

1、Adobe 多款产品存在安全漏洞

Adobe 的 Flash Media Server、Flash Player/AIR 和 ColdFusion 等多款产品存在安全漏洞，攻击者可利用这些漏洞进行拒绝服务攻击或以应用程序权限执行特定代码。具体漏洞信息为：Adobe Flash Media Server 存在可导致拒绝服务攻击的输入验证漏洞、Adobe Flash Media Server 存在可导致拒绝服务攻击的内存耗竭漏洞、Adobe Flash Media Server JS 方法存可导致任意代码执行的漏洞、Adobe Flash Media Server JS 方法存可导致拒绝服务攻击的漏洞、Adobe Flash Player 10.1.53.64/AIR 2.0.2.12610 存在可导致点击劫持攻击的漏洞、Adobe Flash Player 10.1.53.64/AIR 2.0.2.12610 存在多个内存破坏漏洞、Adobe Flash Player 10.1.53.64/AIR 2.0.2.12610 存在未明内存破坏漏洞、Adobe ColdFusion 未明目录遍历漏洞。目前 Adobe 已经发布补丁程序修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01622>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01621>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01620>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01619>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01618>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01617>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01616>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01610>

2、Cisco ACE 和 WCS 存在多个安全漏洞

Cisco 应用控制引擎 (ACE) 是一套负载均衡和应用交付产品组合的解决方案, Cisco 无线控制系统 (WCS) 是支持高性能应用程序和关键任务的解决方案。这两款产品存在多个安全漏洞, 攻击者可利用漏洞执行拒绝服务攻击。具体漏洞包括: Cisco ACE 4710 HTTP、RTSP 和 SIP 检测存在拒绝服务漏洞、Cisco ACE 模块和引擎 RTSP 检测存在拒绝服务漏洞、Cisco ACE 模块和引擎 SIP 检测存在拒绝服务漏洞、Cisco Wireless Control System (WCS) 存在未明 SQL 注入漏洞、Cisco ACE 应用控制引擎模块 SSL 处理存在拒绝服务漏洞。目前 Cisco 已经发布安全公告 (cisco-sa-20100811-wcs) 修复上述安全漏洞, 建议相关用户尽快下载更新。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01638>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01637>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01636>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01635>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01632>

3、Mozilla Bugzilla 存在多个安全漏洞

Mozilla Bugzilla 是一款基于 Web 的 BUG 跟踪系统。Mozilla Bugzilla 存在多个安全漏洞, 攻击者可利用漏洞执行拒绝服务攻击。具体漏洞包括: Bugzilla 的 "sudo" 功能存在漏洞、Bugzilla 处理 Bug 评注时存在漏洞、Bugzilla 的 "Reports" 和 "Duplicates" 页存在漏洞、Bugzilla 布尔图标搜索接口存在漏洞。目前 Bugzilla 3.2.8、3.4.8、3.6.2 和 3.7.3 版本已经修复上述安全漏洞, 建议相关用户尽快下载使用。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01565>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01564>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01562>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01560>

4、Foxit Reader 存在 FreeType2 CFF 字体解析漏洞

Foxit Reader (福昕阅读器) 是一款 PDF 文档阅读器。Foxit Reader 使用 FreeType2 代码解析 CFF 字体某些操作码时存在错误, 攻击者可通过诱使用户打开经特殊构建的 PDF 文件, 以应用程序权限执行任意指令。目前 Foxit Reader 4.1.1 已经修复该漏洞, 建议相关用户尽快下载使用。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01575>

小结: 本周, Adobe 和 Cisco 多款产品、Mozilla BUG 跟踪系统、福昕阅读器均曝出安全漏洞。这些漏洞可被攻击者利用实施远程或本地网络攻击, 对国内相关用户的信息安

全和公共互联网网络安全构成了一定威胁，请使用以上软件的相关机构和个人及时采取安全防范措施。

本周重要的漏洞修补信息

本周，CNVD 整理和发布以下重要安全修补信息。

1、微软发布八月安全公告

8月11日，微软发布八月份的月度安全公告，共包含14个安全公告，其中8个被定义为危害级别最高的“严重”；共修补了34个安全漏洞，修补数量创下微软近年来的历史最高值。修补的漏洞涉及 Windows、IE 浏览器以及 Office 等软件，攻击者可以利用这些漏洞进行拒绝服务、任意代码执行、权限提升等攻击，给众多互联网用户带来严重的安全威胁。CNVD 提醒广大用户为避免遭受漏洞影响请及时下载补丁更新。

补丁下载链接：<http://www.cnvd.org.cn/patch/792>

<http://www.cnvd.org.cn/patch/793>

<http://www.cnvd.org.cn/patch/797>

<http://www.cnvd.org.cn/patch/798>

<http://www.cnvd.org.cn/patch/801>

<http://www.cnvd.org.cn/patch/802>

<http://www.cnvd.org.cn/patch/803>

<http://www.cnvd.org.cn/patch/804>

<http://www.cnvd.org.cn/patch/806>

<http://www.cnvd.org.cn/patch/808>

<http://www.cnvd.org.cn/patch/810>

<http://www.cnvd.org.cn/patch/811>

<http://www.cnvd.org.cn/patch/812>

<http://www.cnvd.org.cn/patch/813>

<http://www.cnvd.org.cn/patch/814>

<http://www.cnvd.org.cn/patch/815>

<http://www.cnvd.org.cn/patch/826>

<http://www.cnvd.org.cn/patch/781>

<http://www.cnvd.org.cn/patch/782>

<http://www.cnvd.org.cn/patch/783>

<http://www.cnvd.org.cn/patch/784>

<http://www.cnvd.org.cn/patch/785>

<http://www.cnvd.org.cn/patch/795>

<http://www.cnvd.org.cn/patch/796>

<http://www.cnvd.org.cn/patch/805>

<http://www.cnvd.org.cn/patch/807>

<http://www.cnvd.org.cn/patch/809>

<http://www.cnvd.org.cn/patch/787>
<http://www.cnvd.org.cn/patch/788>
<http://www.cnvd.org.cn/patch/789>
<http://www.cnvd.org.cn/patch/790>
<http://www.cnvd.org.cn/patch/791>

本周要闻速递

1、Flash Player 被曝至少存在 6 个严重安全漏洞

8 月 12 日消息，据外电报道，Adobe 公司称在 Flash Player 上发现至少 6 个严重安全漏洞，可以允许黑客运行遥控码进行攻击。受这些漏洞影响的版本是 Adobe Flash Player 10.1.53.64 以及早前的版本、Adobe AIR 2.0.2.12610 和较早版本。Windows，Macintosh，Linux 和 Solaris 等系统均受到影响。Adobe 称漏洞的记忆功能可以使应用崩溃，从而允许黑客进行恶意攻击。六个漏洞中的一个可以造成点击劫持攻击。Adobe 建议用户将易受攻击的 Adobe Flash Player 版本更新至 10.1.82.76 版本，Adobe AIR 更新至 2.0.3 版本。

参考链接：<http://www.hackbase.com/news/2010-08-12/37200.html>

2、苹果发布补丁修复 iPhone 和 iPad 安全漏洞

德国联邦信息安全办公室在上周三发布了一篇警告，内容称苹果公司的 iPhone、iPad 以及 iPod Touch 有几个版本都存在严重的安全问题，可能会导致攻击者盗取用户信息。苹果公司很快承认了两个安全漏洞的存在，并对 iOS 4 上的这两个漏洞进行了修复，同时苹果还为 iPad 发布了一个单独的补丁，因为 iPad 平板使用的是 iOS 3.2 版本。据了解，这两个安全漏洞的危害性都比较大，其中一个漏洞能够利用 Safari 浏览器解析 PDF 文件中字体的漏洞攻破这个浏览器，从而使浏览器访问 jailbreakme.com 网站。而第二个漏洞则能够攻破隔离“沙箱”并且得到这种设备的完全控制权或者“根”控制权，这样就能够使苹果设备执行任意代码。

参考链接：<http://price.zol.com.cn/191/1916532.html>

3、Twitter 漏洞导致 140 个字符限制被打破

Twitter 网站规定每条 Twitter 消息长度不得超过 140 个字符，近日有用户发现 Twitter 网站的这一限制性功能存在漏洞，部分用户发布消息的长度远高于此限制字符数。一名 Twitter 日本用户发布了 2135 字的 Twitter 消息，该条消息被超过 100 名其他用户转载。由于元数据（metadata）显示方面的原因，Twitter 超过字符数限制的消息不能在手机上浏览，用户只能通过 Twitter 首页访问到。不过这一缺陷被曝光的数小时后，Twitter 工程师已经修正了长消息发布漏洞。

参考链接：<http://www.cnbeta.com/articles/119354.htm>

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