

信息安全漏洞周报

2010年8月2日-2010年8月8日

2010年第30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 30 个，其中高危漏洞 3 个、中危漏洞 8 个、低危漏洞 19 个。上述漏洞中，可利用来实施远程攻击的漏洞有 29 个。经检测发现，网上已经出现针对“Akamai 下载管理器存在任意文件下载漏洞”的零日攻击代码，请广大用户注意做好相关防护措施。目前，相关厂商已经为 23 个漏洞提供了修补方案，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、Cisco 多个产品存在安全漏洞

Cisco 防火墙服务模块、Cisco 自适应安全设备和 Cisco 无线控制系统均出现安全漏洞，攻击者利用漏洞可进行拒绝服务攻击，并以应用程序权限执行特定代码。具体漏洞包括：Cisco 防火墙 TCP 拒绝服务漏洞、Cisco 防火墙 SunRPC 检测拒绝服务漏洞、Cisco ASA 5500 特殊构建的 IKE 消息拒绝服务漏洞、Cisco ASA 5500 SIP 检测拒绝服务漏洞、Cisco ASA 5500 TLS 传输层拒绝服务漏洞、Cisco SunRPC 检测拒绝服务漏洞、Cisco 无线控制系统跨站脚本漏洞。目前 Cisco 已经发布更新程序修复了上述安全漏洞，建议相关用户尽快下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01549>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01555>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01556>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01557>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01558>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01554>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01559>

2、Adobe Reader/Acrobat 字体解析存在远程代码执行漏洞

Adobe Reader/Acrobat 是 Adobe 公司开发的 PDF 文档阅读/编辑软件。Adobe Reader/Acrobat 在解析 TrueType 字体中“maxp”(Maximum Profile)表的“maxCompositePoints”字段时，CoolType.dll 存在整数溢出错误，攻击者可通过诱使用户打开经特殊构建 TrueType 字体的 PDF 文件，达到破坏用户内存的目的。目前 Adobe 尚未发布相应的升级补丁，建议相关用户继续关注厂商主页以获取修补方案。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01551>

3、Novell iPrint客户端存在多个安全漏洞

Novell iPrint客户端打印解决方案允许用户向网络打印机发送文档，其存在的多个安全漏洞允许攻击者以当前运行浏览器的用户权限执行特定代码。具体漏洞包括：Novell iPrint 客户端浏览器插件CleanUploadFiles函数任意文件删除漏洞、Novell iPrint客户端浏览器插件ExecuteRequest调试参数远程栈溢出漏洞、Novell iPrint客户端浏览器插件运算参数栈溢出漏洞、Novell iPrint客户端浏览器插件参数名溢出漏洞。目前厂商已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-2010-01528>

4、SigPlus Pro ActiveX 控件存在缓冲区溢出漏洞

SigPlus Pro ActiveX控件是一款用于电子签名的应用插件。SigPlus Pro ActiveX控件（SigPlus.ocx）未正确处理传送给LCDWriteString()函数的HexString参数，如果用户受骗访问了恶意网页并传送超长字符串参数便可触发栈溢出，导致执行特定代码。目前SigPlus Pro ActiveX Control 3.95已经修复了该安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01539>

小结：本周CNVD收集的漏洞信息中，除Adobe Reader/Acrobat字体解析存在的远程代码执行漏洞尚未发布补丁或更新程序外，其它漏洞信息已有相应的安全补丁或更新程序。这些漏洞对国内相关用户的信息安全和公共互联网网络安全均构成威胁，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、Microsoft Windows 快捷方式'LNK'文件自动文件执行漏洞的补丁

微软于8月3日发布补丁修复了微软LNK漏洞(快捷方式漏洞)，该漏洞给众多Windows用户带来严重的信息安全威胁，相关的攻击代码在网上快速出现并传播，引发大量的攻击事件。建议广大用户尽快下载安装补丁程序，以避免引发与该漏洞相关的网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patch/745>



本周要闻速递

1、微软 Windows 内核曝漏洞

据国外媒体报道，以色列安全研究人员吉尔·达巴赫近日披露，Windows 内核存在缓冲区溢出漏洞。丹麦安全漏洞跟踪公司 Secunia 称，达巴赫发现的漏洞存在于“Win32k.sys”内核模式设备驱动中，黑客可利用应用程序接口(API)“GetClipboaedData”对用户发动攻击，该漏洞影响多个版本的 Windows 系统，包括 XP SP3、Server 2003 R2、Vista、Windows 7 和 Windows Server 2008 SP2。目前，微软安全部门表示，微软正在调查该问题，待核实后，微软将采取适当措施来保护用户。

参考链接：http://news.ccidnet.com/art/1032/20100808/2145743_1.html

2、德国称苹果 iOS 系统漏洞可导致数据失窃

德国联邦信息安全局发布警告称，一些版本的苹果 iPhone、iPad 和 iPod Touch 可能存在严重安全问题。苹果 iOS 操作系统有两个严重的安全漏洞尚未得到修补，这些安全漏洞能够让攻击者访问整个系统，包括得到管理员权限。如果用户打开一个黑客控制的网站或者一个 PDF 文件，攻击者就能够窃取用户的口令、计划安排、照片、文本消息、电子邮件，甚至能够监听用户的通话。目前，苹果在德国的发言人 Georg Albrecht 表示，苹果正在调查这件事情。

参考链接：<http://www.hackbase.com/news/2010-08-05/36999.html>

3、微软将于 8 月 10 日发布 14 个漏洞补丁修补 34 个漏洞

微软透露，下周二(8月10日)，将公布多达 14 个安全公告，修补 34 个漏洞，这是历史上微软修补漏洞数量最多的一个月，影响的产品包括 Windows, Office, Internet Explorer, SQL 和 Silverlight，而且影响面非常广，从 Windows 7 到 XP, IE6 到 IE8, Office XP 到 2008 for Mac, Microsoft Works 9 和 Silverlight2 和 3 全部中招，因此建议广大用户及时进行系统升级，不过需要注意的是 XP SP2 用户将不会得到任何升级补丁。

参考链接：<http://www.hackbase.com/news/2010-08-06/37034.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