

信息安全漏洞周报

2010 年 5 月 17 日-2010 年 5 月 23 日

2010 年第 20 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)本周共收集和整理信息安全漏洞 50 个,其中高危漏洞 5 个、中危漏洞 5 个、低危漏洞 40 个。上述漏洞中,可利用来实施远程攻击的漏洞有 49 个。经检测发现,网上已经出现针对“nginx 存在文件类型错误解析漏洞”、“IIS 存在源码泄露及文件类型解析错误解析漏洞”、“Joomla 组件 com_konsultasi (sid) SQL 注入漏洞”、“土豆网 callback 参数导致的跨站漏洞”、“Firefox 3.6.3 存在多个远程拒绝服务漏洞”的零日攻击代码,请广大用户注意做好防护措施。目前,相关厂商已经为 27 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、nginx 存在文件类型错误解析漏洞

nginx 是一款高性能 Web 和反向代理服务器软件。nginx 存在一个严重的 0day 漏洞,在默认情况下可能导致服务器错误地将任何类型的文件以 PHP 方式进行解析,恶意攻击者可能利用该漏洞攻陷支持 PHP 的 nginx 服务器。目前厂商尚未发布升级补丁,建议用户可采用以下临时解决方案来避免受到漏洞威胁。更改配置文件: (1) 设置 php.ini 的 cgi.fix_pathinfo 为 0, 重启 php; (2) nginx 的 vhost 配置添加 “if (\$fastcgi_script_name ~ \.*\.*.php) { return 403; }”, 重启 nginx; (3) 禁止上传目录解释 PHP 程序。

参考链接: <http://www.80sec.com/nginx-securit.html>

2、IIS 存在源码泄露及文件类型错误解析漏洞

IIS 是微软推出的一款 Web 服务器软件。名为“80sec”的 WEB 安全研究团体发现 IIS 的较高版本中存在一个严重的安全漏洞,在默认配置情况下可能导致服务器端脚本源码泄露,也可能错误地将任何类型的文件以 PHP 的方式进行解析,恶意攻击者可利用该漏洞攻陷支持 PHP 的 IIS 服务器,特别是虚拟主机用户可能遭受较大影响。目前微软尚未发布补

丁或升级程序，建议相关用户通过关闭 cgi.fix_pathinfo 为“0”的临时解决方案来避免受到漏洞攻击。

参考链接：<http://www.80sec.com/iis-cgifastcgi-security-hol.html>

3、Hitachi 的多个产品存在安全漏洞

Hitachi（日立）公司的多个产品存在安全漏洞。远程攻击者可以利用漏洞以应用程序权限执行任意代码或者进行未授权访问。具体漏洞信息为：Hitachi XMAP3和Hitachi EUR 产品代码执行漏洞、Hitachi Web Server SSL证书撤销安全绕过漏洞、Hitachi TP1/Message Control畸形报文远程拒绝服务漏洞、Hitachi Web Server SSL启用远程拒绝服务漏洞、Hitachi Collaboration Common Utility未明栈缓冲区溢出漏洞。目前厂商已经发布了升级补丁以修复该安全问题，建议相关用户尽快下载使用。

参考链接：<http://www.hitachi.co.jp/Prod/comp/soft1/security/info/>

4、SyncBack 存在缓冲区溢出漏洞

SyncBack是一款专业级的系统备份软件。SyncBack在处理用户配置文件时存在边界错误，攻击者可诱使用户打开特殊构建的恶意.sps文件，导致基于栈的缓冲区溢出。成功地利用该漏洞后，远程攻击者可以以应用程序权限执行任意指令。目前2BrightSparks SyncBack 3.2.21版本已经修复此漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-00960>

5、Microsoft Windows Canonical 显卡驱动存在远程代码执行漏洞

Microsoft Windows Canonical显卡驱动(cdd.dll)存在一个安全漏洞，远程攻击者可利用此漏洞执行任意代码。由于内存的随机性，代码执行成功的机会较小，但成功利用此漏洞进行攻击可造成被攻击系统停止响应或自动重启。此漏洞仅影响使用Aero界面的用户，因此在补丁程序发布之前，建议相关用户暂时禁用Aero界面。

参考链接：<http://www.microsoft.com/technet/security/advisory/2028859.mspx?pf=true>

6、Firefox 3.6.3 存在多个远程拒绝服务漏洞

Mozilla Firefox是一款开源WEB浏览器。Firefox的xul.dll和USP10.dll库中包含的gfxWindowsFontGroup::MakeTextRun函数和DoubleWideCharMappedString类存在多个拒绝服务问题。攻击者通过构建恶意网页，使JavaScript代码创建包含超长字符串元素的数组，并把超长字符串追加到P元素内容之后，在Firefox解析时可导致内存破坏或空指针应用，从而可导致应用程序崩溃。目前厂商尚未提供补丁或者升级程序，建议相关用户继续关注厂商的安全更新。

参考链接：http://www.x90c.org/advisories/firefox_3.6.3_crash_advisory.txt

小结：本周安全团体“80sec”发布了 nginx 和 IIS 的两个 0day 漏洞，其中 nginx 0day 漏洞已经使互联网上的百万服务器受到威胁。此外，Hitachi 公司产品、微软显卡驱动、SyncBack 系统备份等被广泛使用的软件均出现了严重漏洞。这些漏洞可被攻击者利用来执行任意代码或导致主机拒绝服务，对国内网民的上网安全造成严重影响。请使用以上软件的广大用户尽快做好安全防护措施，避免受漏洞的影响。

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、Apple 安全公告 MS10-030 和 MS10-031

Apple 于 5 月 18 日发布 Mac OS X 10.6 和 Mac OS X 10.5 的升级补丁，修复 Mac OS X Java 窗口绘图处理远程代码执行漏洞和 Mac OS X Java mediaLibImage 对象处理远程代码执行漏洞。建议用户尽快下载补丁程序修复漏洞，以避免远程攻击者利用漏洞以应用程序权限执行任意指令。

补丁下载链接：<http://support.apple.com/downloads/>

本周要闻速递

1、64 位版 Win 7 安全漏洞可导致黑客远控系统

5 月 20 日消息，据国外媒体报道，微软正在开发补丁，修正 64 位 Windows 7 图形显示组件中的一处漏洞，攻击者可以利用该漏洞使系统崩溃或远程控制系统。微软称，“尽管存在黑客利用该缺陷远程执行代码的可能性，但是，鉴于代码在内存中的存储位置是随机的，因此这种可能性极低。在大多数情况下，成功利用该缺陷的黑客可能使系统停止响应和自动重启。我们没有接到利用该缺陷攻击的报告。”

参考链接：<http://www.hackbase.com/news/2010-05-21/35395.html>

2、nginx 0day 漏洞致使服务器受到严重威胁

国内顶级安全团队 80sec 于 5 月 20 日下午 6 点发布了一个关于 nginx 的漏洞通告，由于该漏洞的存在，使用 nginx+php 组建的网站只要允许上传图片就可能被黑客入侵。到 5 月 21 日凌晨，nginx 尚未发布修复该漏洞的补丁，已经有一些网站被黑了，80sec 提供了暂时的修复方案，请使用 nginx 的管理员权限尽快修复。

参考链接：<http://www.hackbase.com/news/2010-05-21/35398.html>

3、微软将与政府共享漏洞安全信息

据国外媒体报道，为了使得政府关键信息基础设施免受黑客攻击，微软计划与世界各国政府共享软件漏洞的详细资料。微软这个计划的代号为“Omega”，是一个防御性的信息共享计划（DISP），将为各国政府提供有关微软软件产品漏洞的最新技术水平的信息更新。

参考链接：<http://www.hackbase.com/news/2010-05-20/35373.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