

信息安全漏洞周报

2011 年 10 月 31 日-2011 年 11 月 6 日

2011 年第 44 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**高**。

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 126 个，其中高危漏洞 47 个、中危漏洞 63 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 111 个。本周收录的漏洞中，已有 74 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。本周互联网上出现了针对“NJStar Communicator MINISMTP.exe 堆栈缓冲区溢出漏洞”等高危漏洞的零日攻击代码，请使用相关产品的用户注意加强防范。

重要安全公告发布

CNVD 于 11 月 3 日在官方网站发布了《关于 CNVD 与 WOORYUN 开展漏洞事件推送和处置协作的公告》。公告公布了 CNVD 与国内漏洞社区组织 WOORYUN 依托 CNVD 工作平台以及 CNCERT 全国网络安全事件处置平台开展信息推送与处置协作的情况。

根据协商，CNVD/CNCERT 从 WOORYUN 主要接收和处置涉及我国政府部门，银行、电力、证券、金融、民航、保险、税务、铁路等重要信息系统部门，通信行业单位的信息系统漏洞以及其他有可能造成较大影响的情况。按 CNVD/CNCERT 工作流程，对来源于 WOORYUN 的漏洞/事件，经验证确认后，将收录进 CNVD 漏洞库或 CNCERT 事件库，颁布 CNVD 编号和提交证明或 CNCERT 事件处置编号，同时反馈贡献者 WOORYUN Rank 评分。详情以及更多安全公告可参考链接：

<http://www.cnvd.org.cn/notifications/list>

成员单位报送漏洞统计

本周，共 6 家成员单位和多个合作伙伴/个人报送了本周收录的全部 126 个漏洞（联想网御报送的 1 个漏洞暂未收录），各单位报送情况如表 1 所示。其中，恒安嘉新、启明星

辰、绿盟科技的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
恒安嘉新	65	0
启明星辰	57	0
绿盟科技	56	0
安天实验室	30	1
东软	6	0
安氏领信	2	0
网御星云	1	0
个人上报者	2	2
总计	126（去重）	3

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 WordPress、Linux、Joomla!、IBM、Oracle、Microsoft 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。更多厂商产品数量可参见图 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Wordpress	11	8.7%
2	Linux	4	3.2%
3	Joomla!	4	3.2%
4	Drupal	4	3.2%
5	General Electric	3	2.4%
6	D-Link	3	2.4%
7	HP	3	2.4%
8	Oracle	2	1.6%
9	IBM	2	1.6%
10	Microsoft	1	0.8%
11	其它	89	70.5%

表 2 漏洞产品涉及厂商分布统计表



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、Microsoft Windows 内核 Word 文件处理远程代码执行漏洞（Duqu 病毒相关）

Microsoft Windows 是一款操作系统。本周，微软在其官网发布安全警告称，一个最新发现的 Windows 内核漏洞正在受到“Duqu 病毒”攻击。当用户打开 Word 文档时会感染该病毒，可导致系统执行任意代码。据调查，“Duqu 病毒”是超级工厂病毒的第二代变种。该漏洞主要影响 Windows XP、7、Vista、Server 2008/2003 多个版本。CNVD 对此漏洞的综合评级为“高危”。微软尚未发布该漏洞的补丁程序，但在其官网提供了一个临时解决方案用于封堵利用“Duqu 病毒”进行传播的 Windows 内核漏洞，供 Windows 用户下载使用（参考链接：<http://technet.microsoft.com/en-us/security/advisory/2639658>）。此外，CNVD 提醒相关用户可使用安全防护软件拦截攻击系统漏洞的各类病毒。参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08292>

2、南极星软件 MINISMTP 栈缓冲区溢出漏洞

NJStar Communicator（南极星全球通）是一款提供中、日、韩等亚洲语言支持的应用程序。本周，CNVD 接到国外安全研究者 Dillon Beresford 报送的南极星全球通软件 MINISMTP server 栈缓冲区溢出漏洞。攻击者可以利用漏洞可远程发起攻击，以应用程序上下文执行任意代码，可导致拒绝服务，严重的可获得系统主机管理权限。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响南极星全球通软件和捆绑 Mail Extension 的南极星文字处理软件，并且该程序后台进程在关闭上述应用程序后仍然运行。CNVD 对该漏洞的综合评级为“高危”。厂商尚未发布该漏洞的补丁程序，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-2011-08244>

3、HP OpenView Network Node Manager 安全漏洞

本周，HP 的产品 OpenView Network Node Manager(简称 OVNNM)被披露存在多个远程代码执行漏洞。HP OVNNM 是一款网络管理系统软件。利用上述产品漏洞，攻击者可以 WEB 服务进程上下文执行任意代码。CNVD 收录的相关漏洞包括：HP OpenView Network Node Manager 远程代码执行漏洞（CNVD-2011-08295、CNVD-2011-08294、CNVD-2011-08293）。目前，HP 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/vulnerability/CNVD-2011-08295>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08294>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08293>

4、Linux Kernel 产品安全漏洞

Linux 是一款开源的操作系统。本周，Linux 内核被披露存在多个可本地利用的安全漏洞。攻击者可以利用漏洞提升权限、执行任意代码或获得敏感信息。CNVD 收录的相关漏洞包括：Linux Kernel 'mm/oom_kill.c'整数溢出漏洞、Linux Kernel kexec-tools 信息泄露漏洞（CNVD-2011-08214、CNVD-2011-08213、CNVD-2011-08212）。目前，L

linux 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/vulnerability/CNVD-2011-08327>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08214>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08213>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08212>

5、GE 产品安全漏洞

本周，General Electric 公司多款工业控制系统软件被披露存在安全漏洞。主要涉及产品包括：提供信息高速采集、调度的控制系统软件——Proficy Historian 和提供智能生产解决方案的应用软件——Proficy Plant。利用上述产品漏洞，攻击者可以执行任意代码，导致拒绝服务、获取敏感信息甚至是取得对系统主机的控制权。CNVD 收录的相关漏洞包括：GE Proficy Historian Web 管理跨站脚本漏洞、GE Proficy Plant 应用组件远程栈缓冲区溢出漏洞、GE Proficy Historian 数据归档服务远程缓冲区溢出漏洞。上述漏洞中，“GE Proficy Plant 应用组件远程栈缓冲区溢出漏洞、GE Proficy Historian 数据归档服务远程缓冲区溢出漏洞”的综合评级为“高危”。目前，厂商已经修复上述漏洞，CNVD 提醒 GE 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-2011-08291>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08290>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08289>

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/vulnerability/advancedSearch>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2011-08302	Wireshark ERF 文件解析器缓冲区溢出漏洞	高	Wireshark 1.6.3 或 1.4.10 已经修复此漏洞，建议用户下载使用： http://www.wireshark.org/
CNVD-2011-08298	Cisco Small Business SRP500 系列应用设备 WEB 接口远程命令注入漏洞	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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111102-srp500
CNVD-2011-08286	Joomla Vik Real Estate 组件存在 SQL 盲注漏洞	高	暂无
CNVD-2011-08285	Oracle Hyperion Financial Management 'TList6.ocx' ActiveX 控件不安全方法漏洞	高	暂无

CNVD-2011-08284	JBoss AS 远程代码执行漏洞	高	暂无
CNVD-2011-08283	IBM WebSphere 应用服务器管理控制台信息泄露漏洞	高	暂无
CNVD-2011-08276	Google App Engine Python SDK 'FakeFile' 对象本地安全绕过漏洞	高	Google App Engine 1.5.4 已修复此漏洞，建议用户下载使用： http://code.google.com/appengine/downloads.html
CNVD-2011-08250	PROMOTIC ActiveX 控件 'GetPromoticSite' 方法远程代码执行漏洞	高	暂无
CNVD-2011-08249	Oracle Hyperion Enterprise Performance Management arsqls24.dll 缓冲区溢出漏洞	高	暂无
CNVD-2011-08228	TYP03 RTG 文件扩展 SQL 注入漏洞	高	RTG Files (rtg_files) Extension for TYP03 1.5.2 版本已修复此漏洞，建议用户下载使用： http://typo3.org/extensions/repository/view/rtg_files/1.5.2/
CNVD-2011-08203	D-Link DIR-300 远程代码执行漏洞	高	用户可联系供应商升级到最新的固件版本： http://www.dlink.com/

表 3 部分高危漏洞列表

小结：本周披露的相关漏洞对工业控制系统领域造成了较为严重的威胁。Microsoft Windows 内核存在一个与 Duqu 病毒相关的远程代码执行漏洞，而 Duqu 则是与“震网”病毒（Stuxnet）类似的攻击工业控制系统的恶意代码。目前微软尚未发布该漏洞的补丁程序。GE 产品也被披露存在多个安全漏洞。

此外，NJStar 软件零日漏洞对港澳台地区以及东亚其他地区和国家的用户构成较大威胁。Cisco、IBM、D-Link 的产品对相关企业和个人用户构成较大威胁。请使用上述软件的企业和个人用户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、Google 发布升级程序，修补 Google App Engine 安全漏洞

本周，Google 发布升级程序，修补了 Google App Engine 的安全漏洞。Google Ap

p Engine 是基于 Google 数据中心的开发、托管网络应用程序的平台。攻击者可以利用该产品漏洞创建、覆盖任意文件或在系统上执行任意代码。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/patch/5748>

本周要闻速递

1. 黑客利用 Windows 漏洞传播 Duqu 病毒

据国外媒体报道，微软发布公告称，黑客利用了此前 Windows 操作系统中的未知漏洞传播 Duqu 病毒。一些安全专家表示，这可能导致新一轮大规模黑客攻击。微软称，公司正在努力解决这一问题，并将向用户发布安全升级。据悉，安全软件生产商赛门铁克(Symantec)曾于 10 月称，发现一种神秘的计算机病毒，该病毒代码与此前攻击伊朗核电站的 Stuxnet 病毒相似。全球范围内的各国政府和私人研究人员都在努力分析 Duqu 的根源，初步分析显示，这种病毒是由黑客高手研发，主要攻击核电站、炼油厂及输油管道等重要基础设施系统。

参考链接：http://news.ccidnet.com/art/946/20111102/3059651_1.html

2. iOS5 漏洞致 iPhone4S 耗电快，数周将修复

据国外媒体报道，苹果宣称，搭载 iOS 5 系统的部分 iPhone 手机中电池使用时限大大低于预期，其主要原因还是 iOS 5 的漏洞所致。苹果表示，公司已经发现了一些问题，正是这些问题导致了基于 iOS 5 操作系统的部分 iPhone 手机电池使用时长过短。苹果在声明中称：“一小部分用户已经抱怨基于 iOS 5 设备上的电池使用时长低于预期。我们已经发现了其中的原因，正是 iOS 5 中的一些漏洞影响了电池使用时长，我们将在未来几周内发布更新软件，以修复这一漏洞。”

参考链接：http://news.ccidnet.com/art/945/20111103/3065305_1.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