

信息安全漏洞周报

2012 年 11 月 19 日-2012 年 11 月 25 日

2012 年第 46 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 190 个，其中高危漏洞 67 个、中危漏洞 115 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 186 个。本周收录的漏洞中，已有 105 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“TP-LINK TL-WR841N 路由器存在多个 HTML 注入漏洞”、“Novell File Reporter 'NFRAgent.exe' FILE 任意文件读取漏洞”等的零日攻击代码，请使用相关产品的用户注意加强防范。

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报送了本周收录的全部 190 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、恒安嘉新等单位报送数量较多。此外，恒安嘉新向 CNVD 提交了 3 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	111	0
绿盟科技	76	0
安天实验室	35	0
天融信	19	0
安氏领信	6	0
恒安嘉新	61	3
High-Tech Bridge Security Research	3	0
报送总计	311	3
录入总计	190（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 Mozilla、Moodle、IBM、Novell 多家厂商的产品，部分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	Mozilla	31	16%
2	Moodle	6	3%
3	IBM	6	3%
4	Novell	4	2%
5	Apache	3	2%
6	Drupal	3	2%
7	Neocrome	3	2%
8	Hitachi	2	1%
9	TYPO3	2	1%
10	Cisco	1	1%
11	其它	129	67%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 190 个漏洞。其中操作系统漏洞 1 个，应用程序漏洞 107 个，WEB 应用漏洞 76 个，网络设备漏洞 4 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	1
应用程序漏洞	107
WEB 应用漏洞	76
安全产品漏洞	2
网络设备漏洞	4
数据库漏洞	0

表 3 漏洞按影响类型统计表

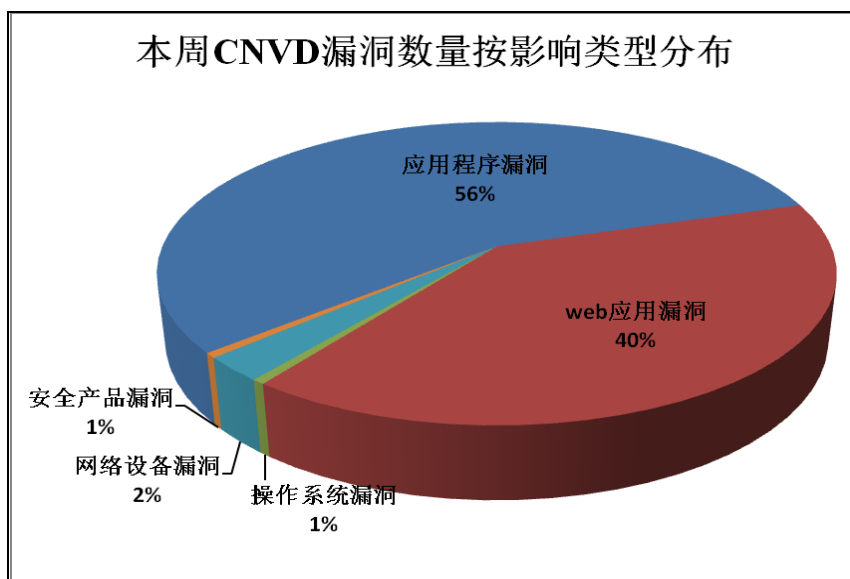


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 4 个网络设备漏洞：多个华为产品本地信息泄露漏洞、多种 Belkin 无线路由器默认 WPA2 密码安全漏洞、TP-LINK TL-WR841N 路由器存在多个 HTML 注入漏洞、Cisco WAG120N 存在多个命令执行漏洞。其中，“Cisco WAG120N 存在多个命令执行漏洞”的综合评级均为“高危”。目前，互联网上已经出现了针对“TP-LINK TL-WR841N 路由器存在多个 HTML 注入漏洞”的攻击代码。相关厂商已经发布了漏洞修补程序。

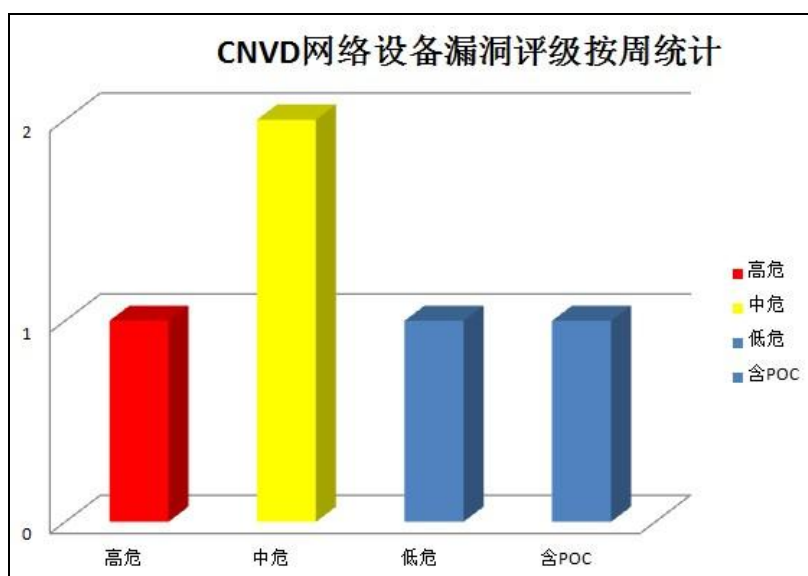


图 2 网络设备漏洞统计

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、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源的 WEB 浏览器。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可构建恶意 WEB 页，诱使用户解析，使应用程序崩溃或执行任意代码。

CNVD收录的相关漏洞包括：Mozilla Firefox osx装载HTML文件堆内存错误引用漏洞、Mozilla Firefox BuildTextRunsScanner::BreakSink::SetBreaks堆内存错误引用漏洞、Mozilla Firefox内存破坏漏洞（CNVD-2012-16031）、Mozilla Firefox nsEditor::FindNextLeafNode堆内存错误引用漏洞、Mozilla Firefox nsWindow::OnExposeEvent堆缓冲区溢出漏洞、Mozilla Firefox nsPlaintextEditor::FireClipboardEvent内存错误引用漏洞、Mozilla Firefox nsViewManager::ProcessPendingUpdates堆内存错误引用漏洞、Mozilla Firefox gfxFont::GetFontEntry内存错误引用漏洞等。上述漏洞的综合评级均为“高危”。厂商已经发布了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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16031

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16008

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16011

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16009

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16006

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16003

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16002

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-15999

2、IBM 产品安全漏洞

IBM WebSphere DataPower XC10 Appliance 是一款结合 DataPower 硬件平台和 IBM 分布式缓存技术的解决方案；IBM Business Process Manager V7.5 是一款集成了以人为中心的业务流程综合 BPM 管理平台。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者利用漏洞可提升权限，执行管理员操作或注入任意 HTML 和脚本代码。

CNVD 收录的相关漏洞包括：IBM WebSphere DataPower XC10 未授权操作漏洞、IBM WebSphere DataPower XC10 远程拒绝服务漏洞、IBM WebSphere DataPower XC10 共享密钥漏洞、IBM Business Process Manager 跨站脚本漏洞、IBM Business Process Manager 'Coaches'跨站脚本漏洞。其中，“IBM WebSphere DataPower XC10 未授权操作漏洞”和“IBM WebSphere DataPower XC10 远程拒绝服务漏洞”的综合评级均为“高危”。厂商已经发布了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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16054

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16055

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16053

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-15960

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-15958

3、SINAPSI eSolar 安全漏洞

Sinapsi eSolar 是一款监控与数据采集(SCADA)产品。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可以以管理员权限访问系统，获得数据库信息或执行任意命令。

CNVD 收录的相关漏洞包括：SINAPSI eSolar Light Photovoltaic System Monitor 页面访问限制漏洞、SINAPSI eSolar Light Photovoltaic System Monitor 默认密码漏洞、SINAPSI eSolar Light Photovoltaic System Monitor SQL 注入漏洞、SINAPSI eSolar Light Photovoltaic System Monitor Shell 命令注入漏洞。上述漏洞的综合评级均为“高危”。目前，厂商已经修复了上述漏洞，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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16047

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16044

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16045

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16046

4、Novell File Reporter 安全漏洞

Novell File Reporter 是 Novell File Management Suite 的一个组件，用于识别网络存储的文件并生成相关使用信息的报告，它由一个中央报告引擎和多个分布式代理(NFR Agent)构成。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可读取任意文件，执行任意代码。

CNVD 收录的相关漏洞包括：Novell File Reporter 'NFRAgent.exe'任意文件上传漏洞、Novell File Reporter 'NFRAgent.exe' FILE 任意文件读取漏洞、Novell File Reporter 'NFRAgent.exe'堆溢出漏洞、Novell File Reporter 'NFRAgent.exe' PATH 任意文件读取漏洞。上述漏洞的综合评级均为“高危”。目前，厂商尚未发布该漏洞的修补程序。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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-15948

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-15951

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-15943

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-15949

5、TP-LINK TL-WR841N 路由器存在多个 HTML 注入漏洞

TP-LINK TL-WR841N router 是一款无线路由器设备。本周，该产品被披露存在多个 HTML 注入漏洞。由于 TP-LINK TL-WR841N 路由器未能正确校验用户提供的输入，远程通过验证的攻击者可以利用漏洞使用 username 或 pwd 参数注入恶意脚本代码，获得敏感信息或劫持用户会话。目前，互联网上已经出现了针对该漏洞的攻击代码，厂商尚未发布该漏洞的修补程序。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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16026

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/publish/main/52/index.html>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2012-16074	tekno.Portal 'anket.php' SQL 注入漏洞	高	暂无
CNVD-2012-16042	HP Integrated Lights-Out 信息泄露漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03515413
CNVD-2012-16049	Yii Framework 'Search'表单字段 SQL 注入漏洞	高	暂无
CNVD-2012-16048	Autonomy Keyview IDOL 存在多个代码执行漏洞	高	Autonomy Keyview IDOL 10.16 已经修复此漏洞，建议用户下载使用： http://www.autonomy.com/content/Products/KeyView/export_sdk.en.html
CNVD-2012-16058	e107 Articulate 'manage_articulate.php'任意文件上传漏洞	高	暂无
CNVD-2012-16071	ExtCalendar 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-16010	dotDefender 模板标签格式串漏洞	高	dotDefender 5.00 已经修复此漏洞，建议用户下载使用： http://www.applicure.com/Products/
CNVD-2012-	Joomla! Odudeprofile 组件 'profession'参数 SQL 注入漏洞	高	暂无

16073			
CNVD-2012-16007	Joomla! jNews 组件 Open Flash Chart 任意文件创建漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.joobi.co/index.php?option=com_content
CNVD-2012-16076	BarCodeWiz ActiveX 控件'Barcode'方法远程缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

小结： 本周，Mozilla Firefox 被披露存在多个漏洞，攻击者利用漏洞可执行任意代码，有可能发起大规模挂马攻击，请广大浏览器用户安装主机防护软件加强防范。IBM 的多款产品也被披露存在漏洞，攻击者可以利用漏洞提升权限，执行管理员操作。SinapsieSolar 和 Novell File Reporter 组件被披露存在多个安全漏洞，利用漏洞可获得数据库信息或执行任意命令。此外，TP-LINK TL-WR841N router 路由设备被披露存在零日漏洞，建议采用该软件的用户随时关注厂商主页，及时获取修复补丁或解决方案。

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、HP 布升级程序，修补 Integrated Lights-Out 漏洞

HP Integrated Lights-Out 用于对服务器的远程管理。本周，HP 修补了 Integrated Lights-Out 存在的信息泄露漏洞。允许攻击者利用漏洞获得敏感信息。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/sites/main/preview/bdgg_preview.htm?tid=25531

本周要闻速递

1. 微软系统漏洞可致用户升级至正版 Win 8

据国外媒体报道，最新发现的系统漏洞使得用户可以通过微软产品更新进程，免费升级至正版 Windows 8 系统。由于采用唯一的激活码，而非此前的批量激活码，盗版制造商一直无法攻陷 Windows 8 系统。但这次发现的系统漏洞使得用户可以通过 KMS（关键管理系统）升级微软媒体中心进而获得免费的正版 Windows 8。整个升级过程所需要的只是一个微软媒体中心升级密钥，这个密钥可以从微软获得。在安装完盗版 Windows 8 后，用户可以进入 KMS 系统，然后输入从微软获得的微软媒体中心升级密钥。由于微软媒体中心在升级中从来不会检测密钥的正确性，用户可以通过微软媒体中心更新激

活 Windows 8。

参考链接: <http://www.enet.com.cn/article/2012/1122/A20121122195411.shtml>

2. Google 承诺修复 Android 4.2 中的日期漏洞

11 月 21 日消息, 对于之前曾有媒体爆料 Android 4.2 新系统中丢失 12 月的日期漏洞, 其内置的标准日期选择控件(date picker)中找不到 12 月份的身影, 现在谷歌公司对外表示他们将会尽快修复这个问题。

参考链接: <http://mobile.qudong.com/2012/1121/128823.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