

信息安全漏洞周报

2013 年 06 月 24 日-2013 年 06 月 30 日

2013 年第 26 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 145 个，其中高危漏洞 58 个、中危漏洞 78 个、低危漏洞 9 个。上述漏洞中，可利用来实施远程攻击的漏洞有 130 个。本周收录的漏洞中，已有 102 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-PS110U 打印服务器'tplink-enum.py'安全绕过漏洞”、“et-chat 权限提升漏洞”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 7 家成员单位及多个合作伙伴和个人报送了本周收录的全部 145 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、天融信、安天实验室、绿盟科技等单位报送数量较多。此外，知道创宇公司和 High-Tech Bridge Security Research Lab 以及个人报送者向 CNVD 提交了 19 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	129	0
绿盟科技	51	0
安天实验室	77	0
天融信	88	0
恒安嘉新	40	0
东软	1	0
知道创宇	3	3

High-Tech Bridge	1	1
天讯瑞达通信技术有限公司	2	0
个人	16	16
报送总计	408	20
录入总计	145（去重）	20

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、Cisco、X.Org、IBM 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	19	13%
2	Cisco	17	12%
3	X.Org	8	6%
4	IBM	5	3%
5	huawei	5	3%
6	Alienvault	4	3%
7	Drupal	3	2%
8	HP	3	2%
9	IceWarp	2	1%
10	Linux	1	1%
11	其它	78	54%

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 145 个漏洞。其中应用程序漏洞 105 个，WEB 应用漏洞 18 个，网络设备漏洞 10 个，操作系统漏洞 4 个，安全产品漏洞 8 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	105
WEB 应用漏洞	18
网络设备漏洞	10
操作系统漏洞	4
安全产品漏洞	8
数据库漏洞	0

表 3 漏洞按影响类型统计表

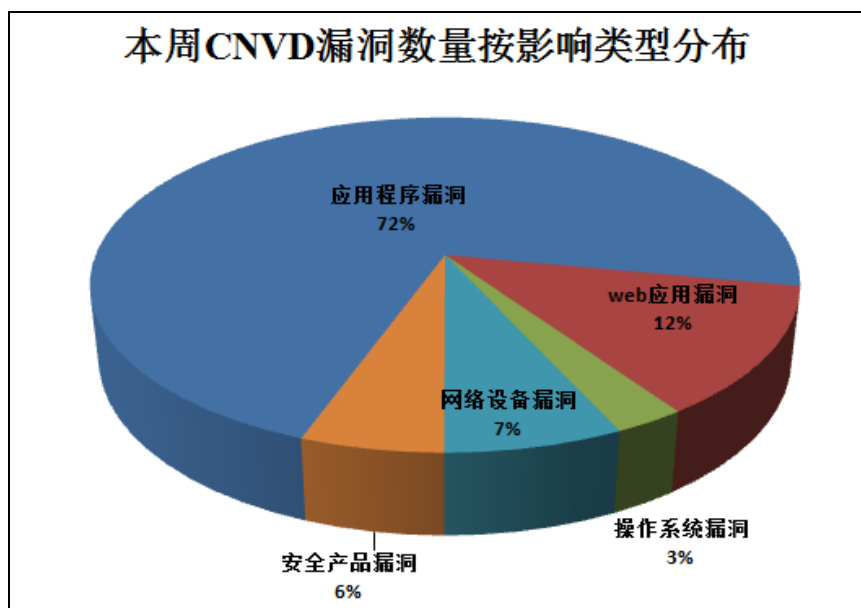


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 10 个网络设备漏洞：Cisco Linksys E1200 N300 Router 'submit_button'参数跨站脚本漏洞、TP-LINK TL-PS110U 打印服务器'tplink-enum.py'安全绕过漏洞、Huawei AR 路由器和交换机 HTTP 模块会话 ID 可预测漏洞、Huawei AR 路由器和交换机 HTTP 模块头字段处理缓冲区溢出漏洞、Huawei AR 路由器和交换机 HTTP 模块缓冲区溢出漏洞、TRENDnet TE100-P1U 存在多个身份验证绕过漏洞、Cisco Linksys X3000 Router 存在多个命令执行漏洞、Cisco Linksys X3000 Router 安全绕过漏洞、Cisco Linksys X3000 Router 存在多个跨站脚本漏洞、ASUS RT-N66U 目录遍历漏洞。

其中，“Huawei AR 路由器和交换机 HTTP 模块会话 ID 可预测漏洞、Huawei AR 路由器和交换机 HTTP 模块头字段处理缓冲区溢出漏洞、Huawei AR 路由器和交换机 HTTP 模块缓冲区溢出漏洞、Cisco Linksys X3000 Router 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“Cisco Linksys E1200 N300 Router 'submit_button'参数跨站脚本漏洞、TP-LINK TL-PS110U 打印服务器'tplink-enum.py'安全绕过漏洞、TRENDnet TE100-P1U 存在多个身份验证绕过漏洞、Cisco Linksys X3000 Router 存在多个命令执行漏洞、Cisco Linksys X3000 Router 存在多个跨站脚本漏洞”的攻击代码。相关厂商已经发布了漏洞修复程序。

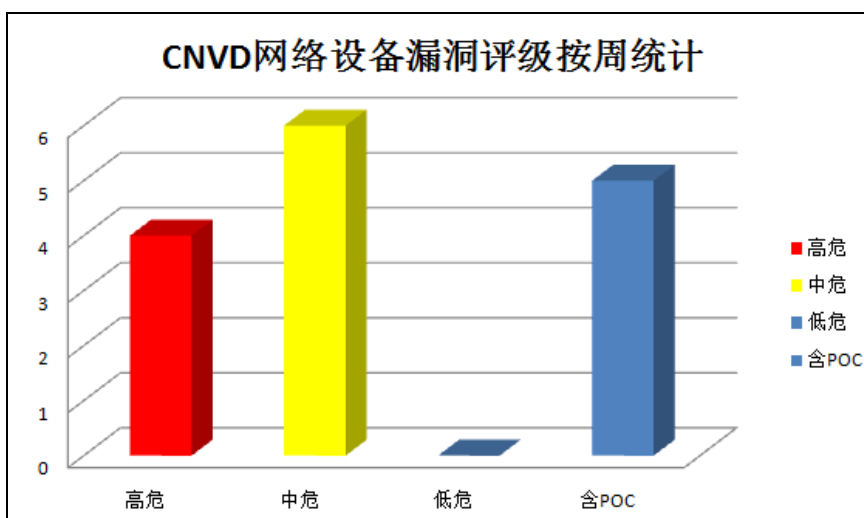


图 2 网络设备漏洞统计

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/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/邮件客户端。本周，上述产品被披露存在多个安全漏洞，远程攻击者利用漏洞可导致应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird 存在多个内存破坏漏洞、Mozilla Firefox/Thunderbird 内存破坏漏洞（CNVD-2013-27553、CNVD-2013-27562）、Mozilla Firefox/Thunderbird CVE-2013-1684 内存错误引用漏洞（CNVD-2013-27564）、Mozilla Firefox/Thunderbird 内存错误引用漏洞（CNVD-2013-27565、CNVD-2013-27566）、Mozilla Firefox/Thunderbird XBL 任意代码执行漏洞、Mozilla Firefox profile 任意代码执行漏洞等。上述漏洞的综合评级均为“高危”。厂商已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/flaw/show/CNVD-2013-27495>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27553>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27562>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27564>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27565>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27566>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27567>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27568>

2、Cisco 产品安全漏洞

Cisco Web Security Appliance 是一款 WEB 网管；Cisco Content Security Management Appliance 是一款内容安全管理应用设备；Cisco Email Security Appliance 是一个 EMAIL 安全网关；Cisco ASA 是一款防火墙设备；Cisco ASA NGFW 是一款扩展 Cisco ASA 平台的附加服务块；Cisco Linksys X3000 是无线路由器产品。本周，上述思科产品被披露存在安全漏洞，攻击者利用漏洞可使设备重载，发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Cisco Web Security Appliance 命令注入漏洞、多个 cisco 产品远程拒绝服务漏洞（CNVD-2013-27587、CNVD-2013-27586）、多个 cisco 产品命令注入漏洞、Cisco ASA NGFW 拒绝服务漏洞、Cisco Linksys X3000 Router 存在多个命令执行漏洞、Cisco Linksys X3000 Router 安全绕过漏洞、Cisco Linksys X3000 Router 存在多个跨站脚本漏洞等。其中，除“Cisco Linksys X3000 Router 安全绕过漏洞”和“Cisco Linksys X3000 Router 存在多个跨站脚本漏洞”，其余漏洞的综合评级均为“高危”。厂商已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/flaw/show/CNVD-2013-27589>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27587>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27586>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27585>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27582>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27351>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27354>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27355>

3、X.Org 产品安全漏洞

X.Org 是 X Window System 的开源实现版本，它支持 Linux、Solaris、以及 BSD 平台。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：X.Org libXp 存在多个远程代码执行漏洞、X.Org libXtst 远程执行代码漏洞、X.Org libXi 'XListInputDevices()'内存破坏漏洞、X.Org libXi 存在多个远程代码执行漏洞、X.Org libXvMC 'XvMCGetDRInfo()'函数远程代码执行漏洞、X.Org libXt '_XtResourceConfigurationEH()'函数远程代码执行漏洞、X.Org libXt 存在多个内存破坏漏洞、X.Org libXv 'XvQueryPortAttributes()'函数远程代码执行漏洞。厂商已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/flaw/show/CNVD-2013-27018>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27019>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27022>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27023>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27024>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27027>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27029>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27030>

4、huawei 产品安全漏洞

Huawei AR routers 和 Huawei S 系列交换机是华为的网络设备；Huawei UTPS 后台软件是运行于 PC 上的管理数据卡的应用软件，提供数据卡的设置、拨号连接、收发短信、管理电话本等功能。本周，上述产品被披露存在多个安全漏洞，远程攻击者利用漏洞可提升权限，劫持会话，执行任意代码。

CNVD 收录的相关漏洞包括：Huawei AR 路由器和交换机 HTTP 模块会话 ID 可预测漏洞、Huawei AR 路由器和交换机 HTTP 模块头字段处理缓冲区溢出漏洞、Huawei AR 路由器和交换机 HTTP 模块缓冲区溢出漏洞、Huawei 多个产品加密不强壮漏洞、Huawei UTPS 后台组件缓冲区溢出漏洞。其中，“Huawei AR 路由器和交换机 HTTP 模块会话 ID 可预测漏洞、Huawei AR 路由器和交换机 HTTP 模块头字段处理缓冲区溢出漏洞、Huawei AR 路由器和交换机 HTTP 模块缓冲区溢出漏洞”的综合评级均为“高危”。厂商已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/flaw/show/CNVD-2013-27266>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27267>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27268>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27269>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27270>

5、et-chat 权限提升漏洞

Et-chat 是一款在线聊天程序。本周，该产品被披露存在一个综合评级为“高危”的权限提升漏洞。Et-chat 未能正确处理 cookie 验证信息，攻击者利用漏洞可提交特殊的 URL，提升权限为管理员权限。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/flaw/show/CNVD-2013-27220>

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/flaw/list.htm>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2013-27549	Kingsoft Spreadsheets etxrw.dll 缓冲区溢出漏洞	高	暂无
CNVD-2013-27412	ClientExec 'index.php' SQL 注入漏洞	高	ClientExec 4.6.5 已经修复此漏洞，建议用户下载更新： https://www.clientexec.com/index.php
CNVD-2013-27440	Seowonintech /cgi-bin/diagnostic.cgi 任意命令执行漏洞	高	暂无
CNVD-2013-27367	MonkeyCMS 远程命令执行漏洞	高	暂无
CNVD-2013-27438	AlienVault OSSIM '/ossim/vulnmeter/index.php'存在多个 SQL 注入漏洞	高	暂无
CNVD-2013-27349	cURL/libcURL 'curl_easy_unescape()'堆内存破坏漏洞	高	cURL 7.31.0 已修复此漏洞，建议用户下载使用： http://curl.haxx.se/
CNVD-2013-27425	aSc Timetables 2013 栈缓冲区溢出漏洞	高	暂无
CNVD-2013-27287	tpp 'exec'任意代码执行漏洞	高	用户可参考如下厂商提供的补丁以修复此漏洞： http://patch-tracker.debian.org/patch/series/view/tpp/1.3.1-3/15-optional-exec.patch https://github.com/xtaran/tpp/commit/350aafbd9a3256f6d479dacb9740bf3f0b9a3fc3
CNVD-2013-27418	PodHawk 任意文件上传漏洞	高	暂无
CNVD-2013-27280	Joomla! RokDownloads 组件任意文件上传漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Mozilla、X.Org 的多款产品被披露存在多个漏洞，攻击者利用漏洞可发起拒绝服务攻击或执行任意代码，可发起大规模的网页篡改和挂马攻击。Cisco、Huawei 的多款设备被披露存在漏洞，攻击者利用漏洞可使设备重载或提升权限。相关企业用户应注意加强防范上述漏洞威胁。此外，Et-chat 被披露存在高危零日漏洞，建议相关用户应随时关注厂商主页，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 发布升级程序，修补多款产品安全漏洞

HP NonStop Server 是一款容错服务器。HP Smart Zero Client 是一款客户端解决方案。本周，HP 发布升级程序，修补了多款产品存在的多个漏洞。攻击者可以利用漏洞绕过安全限制，未经授权访问系统，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/patchInfo/show/34828>
<http://www.cnvd.org.cn/patchInfo/show/34827>
<http://www.cnvd.org.cn/patchInfo/show/34826>

本周要闻速递

1. iOS7 beta 漏洞尚未解决

iOS7 beta 漏洞尚未解决，用户升级需谨慎。之前我们已经提供了 iOS7 beta 版的下载，但是这些版本都只是测试版本，所以有很多漏洞。即便是现在最新的 iOS 7 Beta 2，其 BUG 也是难以忽视。目前，应用重启、假死、发热以及大大小小的多种 BUG 仍然在困扰着部分已经升级了的用户。

参考链接：<http://iphone.265g.com/news/136048.html>

2. Ruby 更新修复了 SSL 中间人漏洞

Ruby 的 OpenSSL 实现绑定版本被发现一个漏洞。该漏洞是因为 X509 名称包含 null 字节的错误解析问题，可导致攻击者放置 "www.ruby-lang.org\0example.com" 这样的证书，并被 Ruby 客户端读取到，然后被解析为 "www.ruby-lang.org"。这使得证书验证程序挂起，同时证书被认定为来自 www.ruby-lang.org。如果攻击者可以获取一个证书包含了 null 字节的 subjectAltName，他们就可以使用这个证书来作为受害者和网站之间的中间人。所有的 Ruby 版本都受此漏洞影响，包括 Ruby 1.8.7 p373 或更早期的版本，Ruby 1.9.3 p447 或更早期版本，以及 Ruby 2.0 p246 和更早期的版本。同时所有 Ruby 源码树中早于 41670 的修订版都存在此问题。请即刻更新到 Ruby 1.8.7 p374, Ruby 1.9.3 p448 和 Ruby 2.0.0 p247。

参考链接：<http://dev.yesky.com/284/35123784.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是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府非盈利的网路安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999