

信息安全漏洞周报

2012 年 7 月 30 日-2012 年 8 月 5 日

2012 年第 31 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 108 个，其中高危漏洞 36 个、中危漏洞 56 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 87 个。本周收录的漏洞中，已有 80 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“Symantec Web Gateway 'deptUploads_data.php' SQL 注入漏洞”、“PHP PDO 内存访问拒绝服务漏洞的验证”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 8 家成员单位和 1 个合作伙伴及个人报送了本周收录的全部 108 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、安天实验室等单位报送数量较多。此外，天融信、上海交通大学以及个人报送者向 CNVD 提交了 9 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	93	0
绿盟科技	74	0
安天实验室	34	0
恒安嘉新	11	0
天融信	19	1
安氏领信	15	0
知道创宇	4	0
东软	3	0

上海交大	1	1
个人	7	7
报送总计	261	0
录入总计	108（去重）	9

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、Microsoft、IBM 等多家厂商的产品，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	Google	15	14%
2	Microsoft	12	11%
3	MIT	3	3%
4	IBM	3	3%
5	RT	3	3%
6	Siemens	3	3%
7	Opera	3	3%
8	Linux	2	2%
9	Mozilla	2	2%
10	Drupal	2	2%
11	其它	60	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 108 个漏洞。其中操作系统漏洞 3 个，应用程序漏洞 76 个，WEB 应用漏洞 22 个，数据库漏洞 1 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	3
应用程序漏洞	76
WEB 应用漏洞	22
网络设备漏洞	4
数据库漏洞	1
安全产品漏洞	2

表 3 漏洞按影响类型统计表

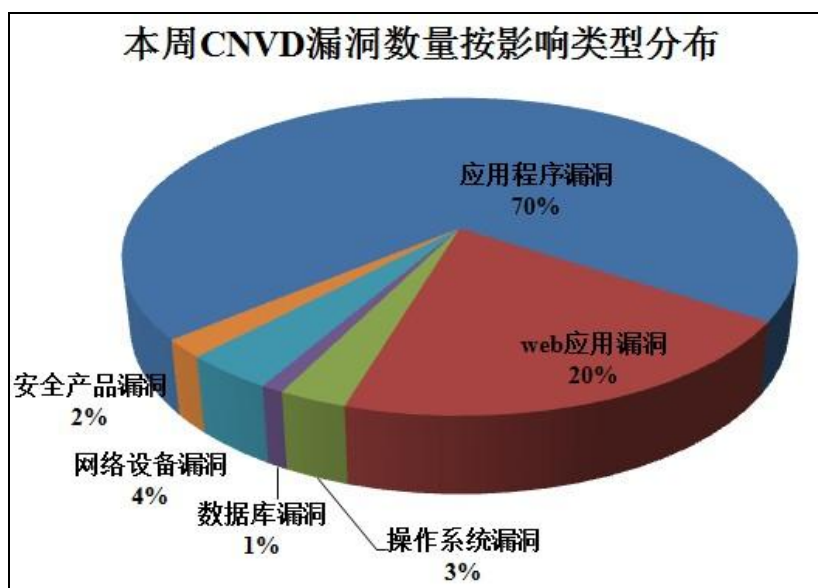


图 1 本周漏洞按影响类型分布

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。“Symantec Web Gateway 'deptUploads_data.php' SQL 注入漏洞、Citrix Access Gateway Plug-in nsepacom ActiveX 控件漏洞（CNVD-2012-13399、CNVD-2012-13400）、Siemens Synco OZW 不安全默认密码漏洞”。上述漏洞的综合评级均为“高危”。其中，Symantec 和 Siemens 的相关产品漏洞可导致网关或网络设备被远程控制，可利用进一步发起针对内部网络的攻击。

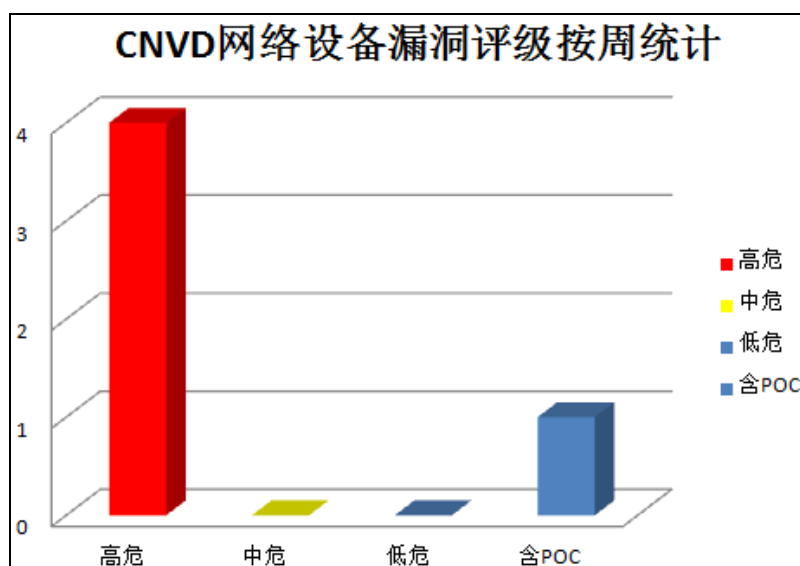


图 2 网络设备漏洞统计



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、Microsoft 产品安全漏洞

Microsoft FAST Search Server 2010 for SharePoint 是一种新的搜索解决方案，它提供了 FAST 以及 Microsoft 的简易性和 TCO；SharePoint Server 是一个服务器功能集成套件，提供全面的内容管理和企业搜索，加速共享业务流程并简化跨界限信息共享。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：Microsoft 多款产品存在漏洞（CNVD-2012-13354、CNVD-2012-13355、CNVD-2012-13353、CNVD-2012-13352、CNVD-2012-13350、CNVD-2012-13341、CNVD-2012-13343、CNVD-2012-13345）等。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=52681
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52682
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52680
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52679
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52677
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52668
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52670
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52672

2、Google Chrome 安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，该产品被披露存在多个安全漏洞，攻击者可利用漏洞使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome CSS DOM 内存错误引用漏洞、Google Chrome PDF 查看器内存错误引用漏洞、Google Chrome PDF 查看器越界写漏洞、Google Chrome PDF 查看器整数溢出漏洞、Google Chrome PDF 处理内存错误引用漏洞（CNVD-2012-13391）、Google Chrome WebP 解码器缓冲区溢出漏洞、Google Chrome date picker 越界访问漏洞、Google Chrome 标签处理拒绝服务漏洞等。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=52916
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52914
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52915
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52906
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52909

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52908

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52912

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52910

3、SIEMENS 产品安全漏洞

Siemens SIMATIC 是一款采用单一工程技术环境的自动化软件。本周，该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。

CNVD 收录的相关漏洞包括：SIEMENS SIMATIC S7-400 拒绝服务漏洞（CNVD-2012-13364）、SIEMENS SIMATIC S7-400 拒绝服务漏洞（CNVD-2012-13363）。上述漏洞的综合评级均为“高危”，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=52776

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52775

4、MIT Kerberos 安全漏洞

Kerberos 是一款使用加密来验证客户端和服务端端的网络协议。本周，该产品被披露存在多个漏洞，远程攻击者利用漏洞使守护进程崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：MIT Kerberos 5 'Kadmin protocol'远程未授权访问漏洞、MIT Kerberos 5 未初始化指针释放远程拒绝服务漏洞、MIT Kerberos 5 未初始化指针引用远程拒绝服务漏洞。其中，“MIT Kerberos 5 未初始化指针引用远程拒绝服务漏洞”和“MIT Kerberos 5 未初始化指针释放远程拒绝服务漏洞”的综合评级均为“高危”，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=52905

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52907

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52903

5、Symantec Web Gateway 'deptUploads_data.php' SQL 注入漏洞

Symantec Web Gateway 是一款 Web 安全网关硬件设备。本周，Symantec Web Gateway 被披露存在一个综合评级为“高危”的 SQL 注入漏洞。由于 Symantec Web Gateway deptUploads_data.php 脚本未能正确处理用户提交给"groupid"的参数，攻击者可以利用漏洞获得数据库敏感信息或控制系统。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=52796

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-2012-13405	Linux Kernel SFC 驱动远程拒绝服务漏洞（CNVD-2012-13405）	高	暂无
CNVD-2012-13406	Open Handset Alliance Android 权限提升漏洞	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://code.google.com/p/android/issues/detail?id=21681
CNVD-2012-13400	Citrix Access Gateway Plug-in nsepacom ActiveX 控件漏洞（CNVD-2012-13400）	高	暂无
CNVD-2012-13416	phpBB 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-13333	IBM Scale Out Network Attached Storage 远程命令执行漏洞	高	IBM Scale Out Network Attached Storage 1.3.2 及之后版本已经修复此漏洞，建议用户下载使用： http://www-03.ibm.com/systems/storage/network/sonas/
CNVD-2012-13408	Joomla! Movm 组件'id' SQL 注入漏洞	高	暂无
CNVD-2012-13368	Empire Server 栈缓冲区溢出漏洞	高	Empire Server 4.3.30 已经修复此漏洞，建议用户下载使用： http://empserver.sourceforge.net/
CNVD-2012-13409	Limny 'escape()' SQL 注入漏洞	高	暂无
CNVD-2012-13410	Ushahidi SQL 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://download.ushahidi.com
CNVD-2012-13370	httpdx 堆溢出漏洞	高	暂无
CNVD-2012-13365	WellinTech KingView 后门未授权访问漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，西门子工业控制系统产品 SIMATIC 被披露存在多个漏洞，可导致系统拒绝服务，影响涉及国内外众多采用该产品的工业行业单位；而国内工业控制系统生产厂商 WellinTech（亚控科技）KingView 被披露存在一个产品后门的情况，目前 CNVD 正进一步跟踪；Microsoft 的多款产品、Google Chrome、MIT Kerberos 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。此外，Symantec Web GatewayWeb 安全网关被披露存在零日漏洞，对相关网络服务器安全构成威胁，需着重加强防范。

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、Mozilla 发布升级程序，修补 Bugzilla 安全漏洞

Mozilla Bugzilla 是一款基于 Web 的 BUG 跟踪系统。本周，Mozilla 发布升级程序，修补了 Bugzilla 存在的漏洞。攻击者可以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=19352
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=19354

本周要闻速递

1. 外媒称 iCloud 漏洞百出 用户随时遭黑客攻击

苹果引以为傲的“安全”又一次惹人笑柄了。虽然 iOS 和 OS X 一直被人们评价为最为安全的操作系统，但是这一次安全问题就出现在连接两个平台的 iCloud 服务之中。根据国外媒体 Wire 的编辑 Mat Honan 透露，他的 iCloud 账户日前遭到黑客的攻击，导致 iPhone、iPad 以及 MacBook Air 被黑客进行远程控制，删除了大量信息。“下午 4:50，有人进入我的 iCloud 账户，重新设置了密码后将确认信息发送至垃圾箱。我的 iCloud 密码由 7 位字母和数字组合，从来没有在其它地方使用过。然后到了下午 5:00，我的 iPhone 资料被远程删除、5:01，iPad 资料被删除、5:05，MacBook Air 同样成为受害者。Honan 称，这似乎不是因为什么技术原因，实际上是那些黑客不知道通过什么手段，说服苹果的技术人员将自己的 iCloud 密码进行了改动，而新密码正中黑客下怀，得以通过 Find my iphone 将与 iCloud 相关的信息进行远程控制。

参考链接：<http://www.hackbase.com/news/2012-08-06/113531.html>

2. 育碧修补 Uplay 漏洞

育碧紧急发布 Uplay 2.0.4 版，力图更正浏览器插件可执行 Uplay 之外应用的漏洞。由于除常规启动程序外，安装例程还为浏览器安装了一个插件，使得外部网站可通过插件漏洞执行访问本机内容。针对该漏洞定制了一个网页，在到访用户没有任何操作的情况下通过浏览器启动了本机的计算器小程序。玩家需启动 AC2、ACR、HAWX 2、断罪、未来战士等育碧作品中的任何一部，让 Uplay 自行修补该漏洞。

参考链接：<http://cpu.zol.com.cn/310/3106757.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