

信息安全漏洞周报

2012 年 4 月 30 日-2012 年 5 月 6 日

2012 年第 18 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**低**。

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 76 个，其中高危漏洞 29 个、中危漏洞 41 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 72 个。本周收录的漏洞中，已有 36 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“Nokia PC Suite Video Manager '.mp4'文件拒绝服务漏洞”、“GENU 存在多个 SQL 注入漏洞”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 家成员单位和多个合作伙伴报送了本周收录的全部 76 个漏洞。各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、天融信等单位报送数量较多。广西网信报送了 5 个原创漏洞，知道创宇报送了 1 个原创漏洞，个人上报者报送了 2 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	107	0
启明星辰	58	0
天融信	35	0
恒安嘉新	22	0
安天实验室	11	0
安氏领信	4	0
东软	4	0
奇虎	1	0
知道创宇	1	1

广西网信	5	5
个人上报者	2	2
报送总计	250	8
录入总计	76（去重）	8

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 HP、WordPress、Google、Drupal 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	HP	13	17.1%
2	WordPress	8	10.5%
3	Google	5	6.6%
4	Drupal	4	5.3%
5	Alienvault	2	2.6%
6	MyClientBase	2	2.6%
7	eFront	2	2.6%
8	Microsoft	1	1.3%
9	Oracle	1	1.3%
10	Citrix	1	1.3%
11	其它	37	48.8%

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 76 个漏洞。其中操作系统漏洞 1 个，应用程序漏洞 41 个，WEB 应用漏洞 33 个，数据库漏洞 1 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	41
WEB 应用漏洞	33
网络设备漏洞	0
数据库漏洞	1
安全产品漏洞	0

表 3 漏洞按影响类型统计表

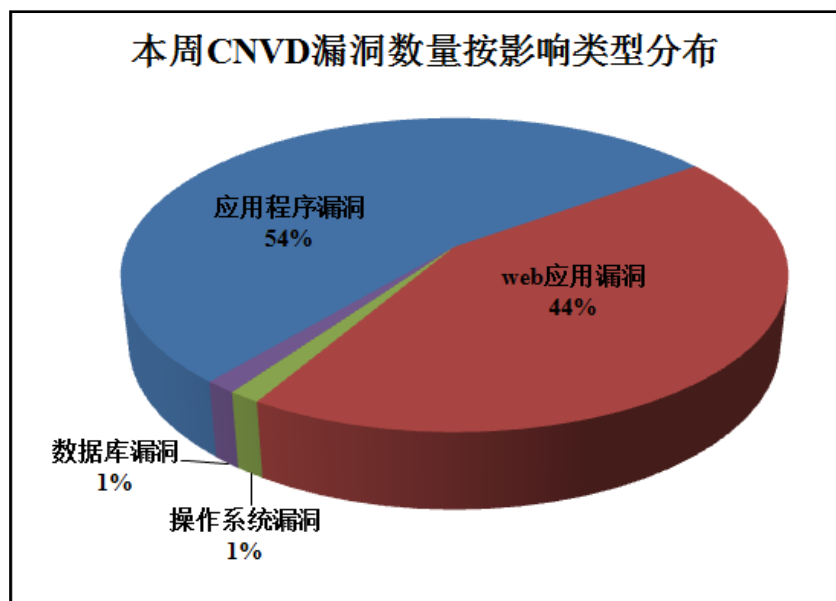


图 1 本周漏洞按影响类型分布

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、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，攻击者可以利用漏洞构建恶意 WEB 页，诱使用户解析执行任意代码。CNVD 收录的相关漏洞包括：Google Chrome XML 解析漏洞、Google Chrome floats 处理漏洞（CNVD-2012-11563）、Google Chrome 沙盒 IPC 竞争条件漏洞、Google Chrome IPC 校验失败漏洞、Google Chrome floats 处理内存错误引用漏洞。上述漏洞的综合评级均为“高危”。目前，厂商已经发布这些漏洞的修补程序，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=48322
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48321
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48320
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48318
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48319

2、HP 产品安全漏洞

HP Systems Insight Manager 是一款实现对 IT 基础设施统一管理的解决方案；HP System Health Application 和 Command Line Utilities 是运行在 Linux 上基于 IPMI 的硬件监控工具集；HP SNMP Agents 则是基于 SNMP 协议书的设备监控软件。本周，上述 HP 产品被披露存在多个安全漏洞，攻击者可以利用漏洞构建恶意链接，诱使用户解析，重定向用户到任意 WEB 站点，达到未经授权访问系统资源、窃取敏感信息或执行任意代

码的攻击目的。

CNVD 收录的相关漏洞包括：HP SNMP Agents 存在未明 URI 重定向漏洞、HP System Health Application 和 Command Line Utilities 远程代码执行漏洞、HP SNMP Agents 存在未明跨站脚本漏洞、HP Insight Management Agents 未授权操作数据漏洞、HP Insight Management Agents 跨站脚本漏洞、HP Insight Management Agents URL 重定向漏洞、HP Insight Management Agents 跨站请求伪造漏洞、HP Systems Insight Manager 验证绕过漏洞等。

其中，“HP System Health Application 和 Command Line Utilities 远程代码执行漏洞”、“HP Insight Management Agents URL 重定向漏洞”、“HP Systems Insight Manager 验证绕过漏洞”的综合评级均为“高危”。目前，HP 已经发布这些漏洞的修补程序，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=48375
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48370
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48367
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48366
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48364
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48362
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48361
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48323

3、WordPress 安全漏洞

WordPress 是一款 PHP 语言开发的网站内容管理系统。本周，该产品被披露存在多个安全漏洞，攻击者可以利用漏洞窃取敏感信息或执行任意代码。CNVD 收录的相关漏洞包括：WordPress Zingiri 网上商店插件 HTML 注入漏洞（CNVD-2012-11631）、WordPress wp-comments-post.php 跨站脚本漏洞、WordPress wp-includes/formatting.php 跨站脚本漏洞、WordPress 预先访问限制策略绕过漏洞、WordPress 同源策略绕过漏洞、WordPress js 文件存在未知漏洞、WordPress 插件 WPSC MijnPress 'rwflush'参数跨站脚本漏洞、WordPress swf 文件存在未知漏洞。其中，“WordPress js 文件存在未知漏洞”和“WordPress swf 文件存在未知漏洞”的综合评级为“高危”。目前，除“WordPress 插件 WPSC MijnPress 'rwflush'参数跨站脚本漏洞”和“WordPress Zingiri 网上商店插件 HTML 注入漏洞（CNVD-2012-11631）”外，厂商已经发布其他漏洞的修补程序，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=48396
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48371
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48369
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48368

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48365

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48363

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48356

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48360

4、Drupal 产品安全漏洞

Drupal 是一款网站内容管理系统。本周，该产品的多个模块被披露存在多个安全漏洞，攻击者可以利用漏洞在用户浏览器中执行任意脚本代码，窃取基于 cookie 的身份验证凭据并发起其他攻击。CNVD 收录的相关漏洞包括：Drupal Taxonomy Grid : Catalog 模块存在未明跨站脚本漏洞、Drupal Addressbook 模块 SQL 注入漏洞、Drupal Addressbook 模块跨站脚本漏洞、Drupal Addressbook 模块跨站请求伪造漏洞。其中，“Drupal Addressbook 模块 SQL 注入漏洞”的综合评级为“高危”。厂商尚未发布上述漏洞的修补程序，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=48395

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48391

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48390

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48388

5、GENU 存在多个 SQL 注入漏洞

GENU 是一款网站内容管理系统。本周，GENU 被披露存在一个综合评级为“高危”的 SQL 注入漏洞，主要影响 2012.3 版本。攻击者可以利用漏洞提交恶意 SQL 查询，获得数据库信息或控制应用系统。目前，厂商尚未发布该漏洞的修补程序，且互联网上已经出现了针对该漏洞的攻击代码。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=48317

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-2012-11594	dhcpcd 远程栈缓冲区溢出漏洞（CNVD-2012-11594）	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免可溢出栈： http://roy.marples.name/projects/dhcpcd
CNVD-2012-11593	Citrix Provisioning Services Server 远程代码执行漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免远程攻击者可以利用此漏洞执行任意代码： http://support.citrix.com/article/CTX133039
CNVD-2012-11618	Opial SQL 注入漏洞	高	暂无

CNVD-2012-11616	MyClientBase SQL 注入漏洞	高	暂无
CNVD-2012-11576	WellinTech KingView DLL 装载任意代码执行漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者构建恶意文件，存放在远程 WebDAV 或 SMB 共享上，诱使用户解析，可以应用程序上下文装载恶意库： http://en.wellintech.com/news/detail.aspx?contentid=168
CNVD-2012-11612	OSSIM SQL 注入漏洞	高	暂无
CNVD-2012-11558	DEDECMS SQL 注入漏洞（CNVD-2012-11558）	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者获得数据库信息或控制应用系统： http://www.dedecms.com
CNVD-2012-11607	LAN Messenger 畸形报文远程拒绝服务漏洞	高	暂无
CNVD-2012-11581	Remote-Anything Player '.flm'文件拒绝服务漏洞	高	暂无
CNVD-2012-11579	Samsung NET-i Viewer 'msls31.dll' ActiveX 缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Google Chrome 浏览器以及 HP 的多款产品被批露存在漏洞，攻击者可以利用漏洞构建恶意链接发起攻击。Drupal 和 WordPress 软件等网站内容管理系统被批露存在多个漏洞，攻击者可以利用漏洞窃取敏感信息或执行任意代码。上述产品由于采用的企业和个人用户较多，需引起重视，加强防范。此外，国产网站内容管理系统 DEDECMS 以及国内工业控制系统软件 Kingview 被披露的高危漏洞对国内企业、个人用户造成较大的影响，不过相关厂商都及时提供了补丁或解决方案。

CNVD 提醒使用上述软件的相关机构和个人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、Oracle 发布升级程序，修补 Database 安全漏洞

本周，Oracle 发布升级程序，修补了 Database 存在的安全漏洞。Oracle Database 是一款商业性质的大型数据库。Oracle Database 被披露存在一个“TNS Listener Poison Attack”漏洞，攻击者可以利用漏洞绕过验证，操作 TNS Listener 的数据。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=16602

本周要闻速递

1. 最新的 PHP 补丁未能修复漏洞

据报道, 一个 PHP 远程代码执行漏洞被意外公开在网上, 引发了利用此漏洞对大量网站实施入侵的恐慌。该漏洞可以追溯到 2004 年, 在最近的 CTF 比赛中被暴露。当 PHP 以 CGI 模式运行时 (如 Apache 的 mod_cgid), php-cgi 会接受处理一个查询字符串作为命令行参数以开启某些功能。如 -s, -d 或 -c 传递给 php-cgi, 此处存在的漏洞可以允许攻击者查看源码或进行任意代码执行。PHP 开发者向 PHP 5.3.12 和 5.4.2 发布了补丁, 但很快被发现补丁并未能真的修补该漏洞。

参考链接: <http://www.cnbeta.com/articles/185944.htm>

2. 甲骨文 oracle 漏洞 4 年未修复

最新消息, 甲骨文 Oracle 紧急发布了一个安全公告, 而这个威胁来自于其旗舰版数据库服务器产品的安全漏洞。而这个所谓的 “0-day” 漏洞, 被揭露 4 年前已经被发现, 至今, 甲骨文都未修复, 仅仅给出了一个变通方案。早在 2008 年, 这个漏洞最先由研究员 Joxean Koret 提交给甲骨文 Oracle, 该漏洞允许攻击者劫持客户端和数据库之间的交流信息。据安全公司报告, 有一些需要注意的事项, 报告里还包含了一些技术措施, 可以有效的抵御所有基于此漏洞的攻击。

参考链接: <http://sec.chinabyte.com/264/12326764.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