国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 04 月 04 日-2016 年 04 月 10 日　　2016 年第 15 期

本周漏洞态势研判情况

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 106 个，其中高危漏洞 34 个、中危漏洞 59 个、低危漏洞 13 个。漏洞平均分值为 5.64 分。本周收录的漏洞中，涉及 0day 漏洞 8 个（占 8%）。其中互联网上出现“DotCMS SQL 注入漏洞、Hexchat IRC Client 栈缓冲区溢出漏洞”等零日代码攻击漏洞，请使用相关产品的用户注意加强防范。此外，本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 742 个，与上周（758 个）环比持平。

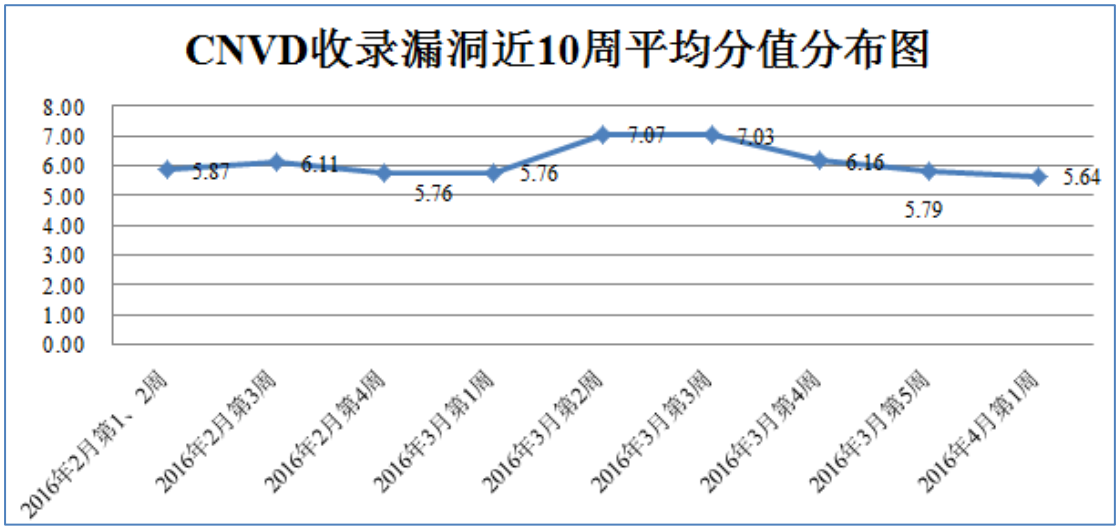

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 8 家成员单位、合作伙伴及个人报送了本周收录的全部 106 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、恒安嘉新、绿盟科技等单位报送数量较多。补天平台、乌云、漏洞盒子、北京国舜科技股份有限公司、腾讯电脑管家、High-Tech

Bridge Security Research Lab、分中心及白帽子向 CNVD 提交了 742 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎(补天平台)	268	268
启明星辰	137	2
安天实验室	115	0
恒安嘉新	93	0
绿盟科技	47	0
杭州安恒信息技术有限公司	45	0
天融信	42	0
H3C	5	0
High-Tech Bridge Security Research Lab	1	1
乌云	396	396
漏洞盒子	39	39
北京国舜科技股份有限公司	1	1
腾讯电脑管家	9	9
CNCERT 福建分中心	2	2
个人	24	24
报送总计	1224	742
录入总计	106（去重）	742

表 1 成员单位上报漏洞统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 106 个漏洞。其中应用程序漏洞 59 个，操作系统漏洞 41 个，Web 应用漏洞 2 个，网络设备漏洞 2 个，安全产品漏洞 2 个。本周，操作系统厂商发布例行月度安全公告，导致操作系统漏洞占比较大。

漏洞影响对象类型	漏洞数量
应用程序漏洞	59
操作系统漏洞	41
Web 应用漏洞	2
网络设备漏洞	2
安全产品漏洞	2

表 2 漏洞按影响类型统计表

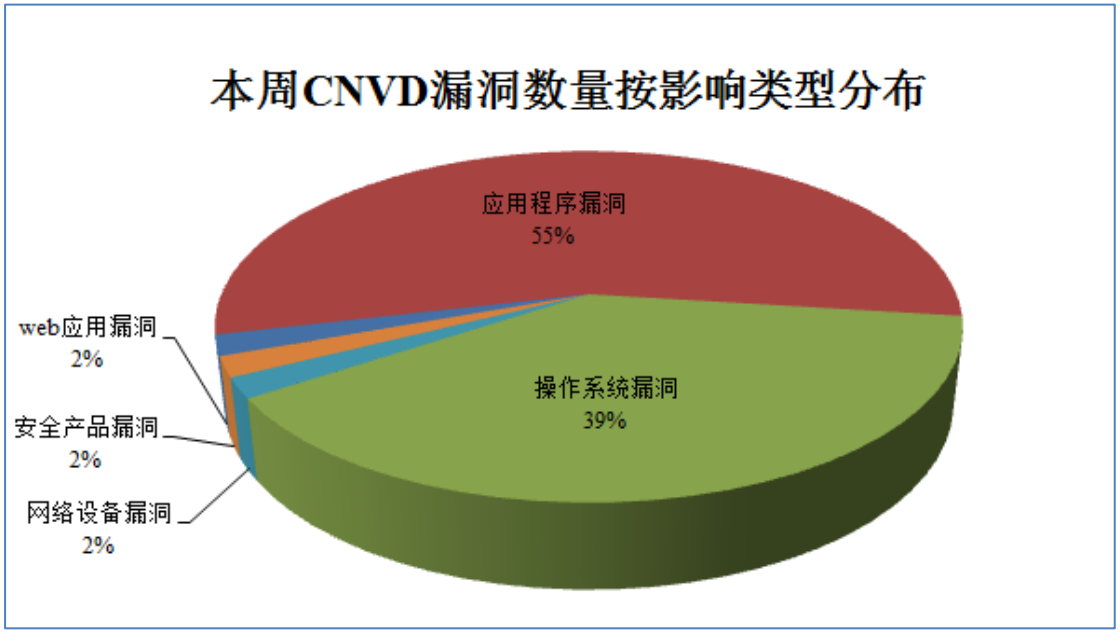

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Linux、Cisco 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Google	28	26%
2	Linux	8	7%
3	Cisco	6	6%
4	IBM	6	6%
5	Red Hat	5	5%
6	Palo Alto Networks	4	4%
7	Pro-face	4	4%
8	imlib2	3	3%
9	Adobe	3	3%
10	其他	39	36%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 5 个电信行业漏洞、29 个移动互联网漏洞、6 个工控系统行业漏洞（如下图所示）。其中，“Android 远程代码执行漏洞、Android Setup Wizard 权限提升漏洞（CNVD-2016-02039）、Android Bluetooth 权限提升漏洞（CNVD-2016-02052）、Android libstagefright 远程代码执行漏洞、Android Mediaserver 远程代码执行漏洞（CNVD-2016-02058、CNVD-2016-02059、CNVD-2016-02060、CNVD-2016-02061、CNVD-2016-02062、CNVD-2016-02063、CNVD-2016-02064）、IBM Tivoli Storage Manager FastBack 缓冲区溢出漏洞（CNVD-2016-02019、CNVD-2016-02020、CNVD-2016-02021、CNVD-2016-02022）”的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

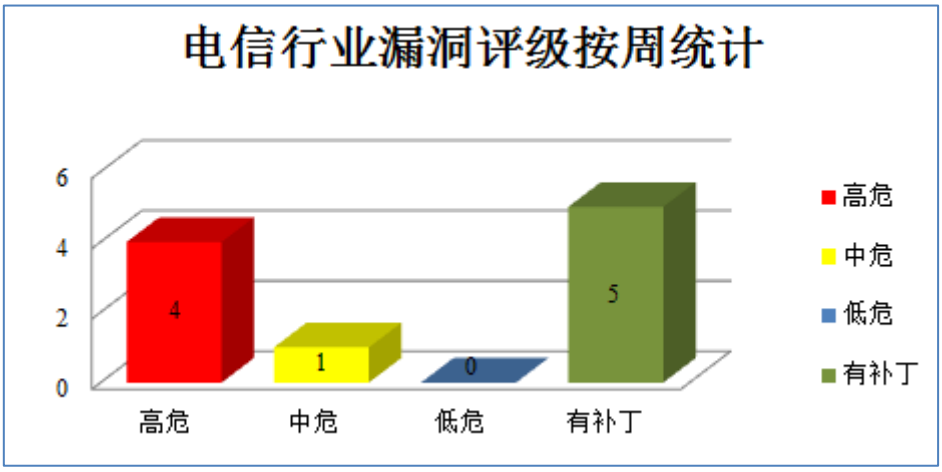

图 3 电信行业漏洞统计

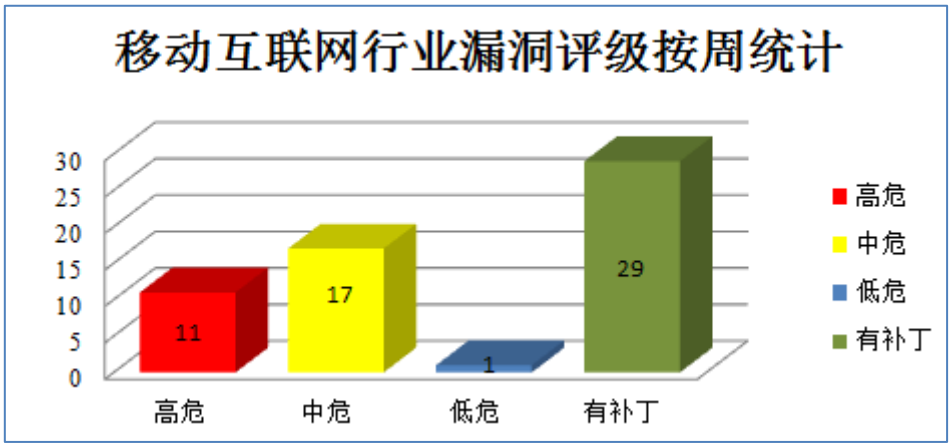

图 4 移动互联网行业漏洞统计

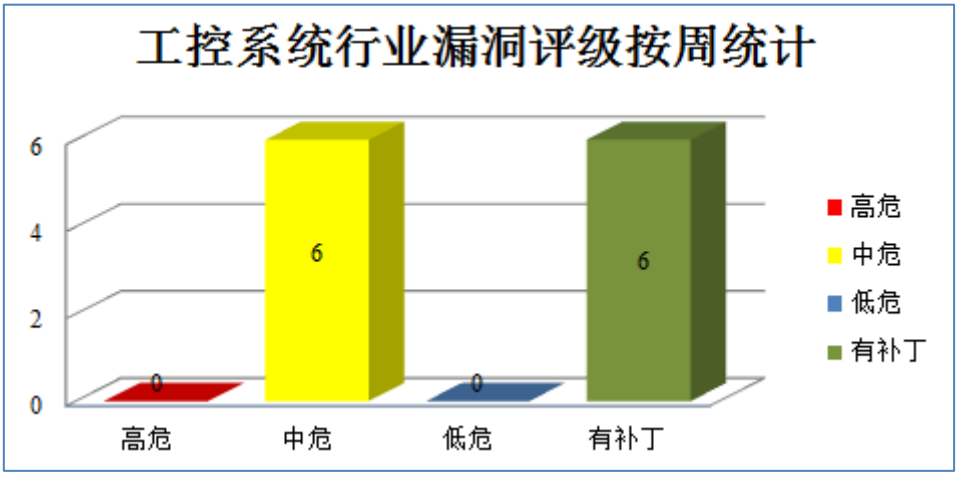

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、 Google 产品安全漏洞

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。Mediaserver 是其中的一个多媒体服务组件。本周，该产品被披露存在信息泄露和远程代码执行漏洞，允许攻击者利用漏洞获取敏感信息和执行任意代码。

CNVD 收录的相关漏洞包括：Android Mediaserver 远程代码执行漏洞（CNVD-2016-02058、CNVD-2016-02059、CNVD-2016-02060、CNVD-2016-02061、CNVD-2016-02062、CNVD-2016-02063、CNVD-2016-02064）、Android Mediaserver 信息泄露漏洞（CNVD-2016-02056）等。其中，除“Android Mediaserver 信息泄露漏洞（CNVD-2016-02056）”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，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-2016-02058

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02059

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02060

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02061

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02062

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02063

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02064

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02056

2、 IBM 产品安全漏洞

IBM Tivoli Storage Manager FastBack 是美国 IBM 公司的一套为 Microsoft Windows 和 Linux 服务器提供持续数据保护和恢复管理功能的软件。IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。本周，上述产品被披露存在缓冲区溢出、绕过限制和拒绝服务漏洞，允许攻击者利用漏洞执行任意代码、绕过限制和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM Tivoli Storage Manager FastBack 拒绝服务漏洞、IBM Maximo Asset Management SHIPREC 绕过限制漏洞、IBM Tivoli Storage Manager FastBack 缓冲区溢出漏洞（CNVD-2016-02019、CNVD-2016-02020、CNVD-2016-02021、CNVD-2016-02022）。其中，除“IBM Tivoli Storage Manager FastBack 拒绝服务漏洞、IBM Maximo Asset Management SHIPREC 绕过限制漏洞”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，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-2016-02023

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02024

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02019

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02020

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02021

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02022

3、Red Hat 产品安全漏洞

Red Hat Network Satellite（RHN Satellite，红帽网络卫星）是美国红帽（Red Hat）公司的一套系统管理平台。该平台可用于扩展 Linux 基础架构，并提供系统管理功能，如管理、配置和监控。本周，该产品被披露存在跨站脚本漏洞，允许攻击者可利用漏洞注入任意 Web 脚本或 HTML。

CNVD 收录的相关漏洞包括：Red Hat Network Satellite 跨站脚本漏洞、Red Hat Network Satellite 跨站脚本漏洞（CNVD-2016-01991、CNVD-2016-01992、CNVD-2016-01993、CNVD-2016-01994）。目前，厂商已经发布了“Red Hat Network Satellite 跨站脚本漏洞”的修补程序。CNVD 提醒用户及时下载补丁更新，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-2016-01995

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01991

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01992

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01993

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01994

4、Cisco 产品安全漏洞

Cisco UCS Invicta 是美国思科（Cisco）公司的一套行业领先的操作软件，专用于使用 NAND 闪存保持高吞吐量、高每秒 I/O 操作（IOPS）率和超低延迟。Cisco TelePresence Server on Mobility Services Engine（MSE）是美国思科（Cisco）公司的一套运行于提供 Wi-Fi 服务的平台（移动服务引擎）Cisco MSE 上的视频会议解决方案。Cisco Prime Infrastructure 是美国思科（Cisco）公司的一套通过 Cisco Prime LAN Management Solution（LMS）和 Cisco Prime Network Control System（NCS）技术进行无线管理的解决方案。Cisco TelePresence 是思科网真解决方案。本周，上述产品被披露存在权限提升、任意代码执行和拒绝服务漏洞，攻击者利用漏洞可提升权限、执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Mobility Services Engine TelePresence Server 拒绝服务漏洞、Cisco UCS Invicta C3124SA Appliance 权限提升漏洞、Cisco Prime Infrastructure 和 Cisco Evolved Programmable Network Manager 任意代码执行漏洞、Cisco TelePresence Server 拒绝服务漏洞、Cisco Prime Infrastructure 权限提升漏洞（CNVD-2016-02072）、Cisco TelePresence Server 拒绝服务漏洞（CNVD-2016-02065）。其中，除“Cisco Prime Infrastructure 权限提升漏洞（CNVD-2016-02072）”外，其余漏洞的综合评级为“高危”。目前，厂商已发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，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-2016-02077
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02076
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02075
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02067
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02072
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02065

5、DotCMS SQL 注入漏洞

DotCMS 是美国 DotCMS 公司的一套内容管理系统（CMS）。该系统支持 RSS 订阅、博客、论坛等模块，并具有易于扩展和构建的特点。本周，DotCMS 被披露存在 SQL 注入漏洞，攻击者可利用漏洞执行任意 SQL 命令。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-2016-02029

更多高危漏洞如表 4 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-2016-01988	PHP WDDX 扩展 wddx.c 缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：

			http://git.php.net/?p=php-src.git;a=commit;h=b1bd4119bcafab6f9a8f84d92cd65eec3afeface
CNVD-2016-01999	Adobe Experience Manager 存在未明漏洞	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：https://helpx.adobe.com/security/products/experience-manager/apsb16-05.html
CNVD-2016-02002	Adobe Experience Manager Dispatcher 安全绕过漏洞	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：https://helpx.adobe.com/security/products/experience-manager/apsb16-05.html
CNVD-2016-02000	HID VertX/Edge 命令注入远程代码执行漏洞	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.hidglobal.cn/products/controllers/vertx
CNVD-2016-02003	HPE Asset Manager 任意代码执行漏洞	高	HP 已经为此发布了一个安全公告（HPSBGN03567）以及相应补丁：https://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05064889
CNVD-2016-02011	Palo Alto Networks PAN-OS 命令注入漏洞（CNVD-2016-02011）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://securityadvisories.paloaltonetworks.com/Home/Detail/35
CNVD-2016-02027	Slackware mercurial 数据包任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://slackware.com/
CNVD-2016-02026	Slackware mercurial 数据包任意代码执行漏（CNVD-2016-02026）	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://slackware.com/
CNVD-2016-02025	Slackware mercurial 数据包任意代码执行漏（CNVD-2016-02025）	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://slackware.com/
CNVD-2016-02034	Palo Alto Networks PAN-OS 命令注入漏洞（CNVD-2016-02034）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://securityadvisories.paloaltonet

			works.com/Home/Detail/36

表 4 部分重要高危漏洞列表

小结：本周，Google 产品被披露存在信息泄露和远程代码执行漏洞，允许攻击者利用漏洞获取敏感信息和执行任意代码。此外，IBM、Red Hat、Cisco 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息、进行跨站脚本攻击、执行任意代码、提升权限和发起拒绝服务攻击等。本周，包括 PHP、Palo Alto 等广泛应用的中间件、设备被披露存在高危漏洞，影响面也较为广泛。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周漏洞要闻速递

1. 微软最新账户身份验证漏洞

英国安全顾问 Jack Whitton 在微软的身份验证系统中发现了一个重要漏洞，攻击者可访问用户的 Outlook、Azure 和 Office 账户，为此微软支付了 1.3 万美元奖金。该漏洞与 Wesley Wineberg 发现的“OAuth CSRF in Live.com”漏洞类似，唯一的不同在于该漏洞影响的是微软的主身份验证系统，而不是 OAuth 保护机制。

参考链接：http://www.freebuf.com/vuls/100912.html

2. 思科 FirePower 系列防火墙存在漏洞，允许恶意软件绕过检测

思科正在发布安全更新程序来修复一个关键漏洞（CVE-2016-1345），该漏洞影响思科公司其中一个最新产品——FirePower 防火墙。该漏洞为 Check Point 的安全研究人员率先发现。根据思科发布的安全公告表示，攻击者可以远程利用该漏洞来允许恶意软件绕过检测。思科将该漏洞级别标注为“高危漏洞”，因此它及时发布了解决 Cisco Firepower 系统软件 5.4.0.7 及更高版本，5.4.1.6 及更高版本和 6.0.1 及更高版本的安全补丁。

参考链接：http://www.freebuf.com/vuls/100842.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

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等

工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999