国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 05 月 22 日-2017 年 05 月 28 日 **2017 年第 22 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 363 个，其中高危漏洞 145 个、中危漏洞 186 个、低危漏洞 32 个。漏洞平均分值为 6.41。本周收录的漏洞中，涉及 0day 漏洞 60 个（占 17%），其中互联网上出现“Moxa AWK-3131A Wireless Access Point 跨站脚本漏洞、Private Tunnel 拒绝服务漏洞”等零日代码攻击漏洞。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 561 个，与上周（608）环比下降 7%。

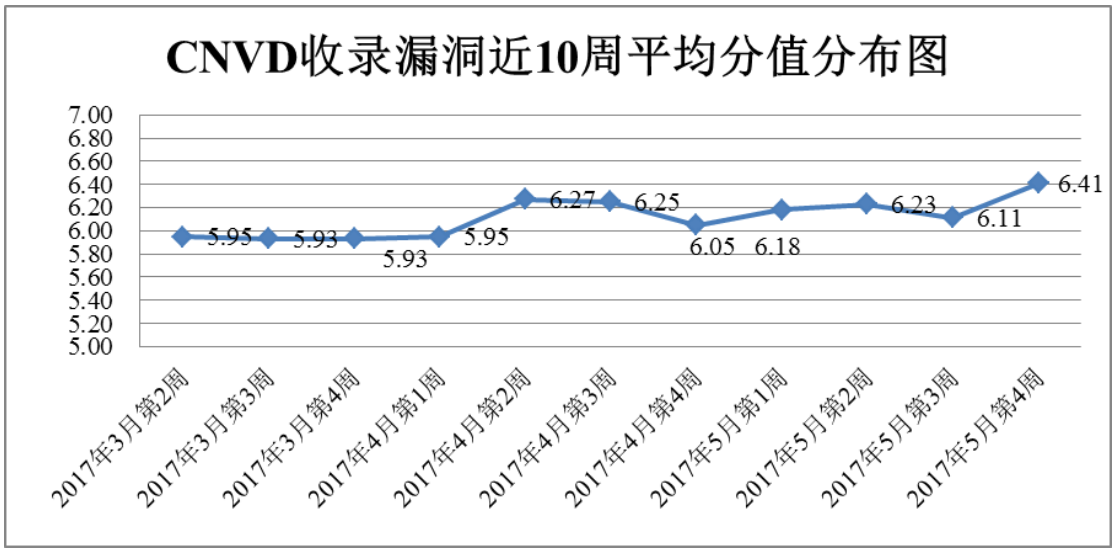

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 14 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 18 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 331 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 89

起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 11 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

郑州微厦计算机科技有限公司、安徽讯飞皆成软件技术有限公司、惠普公司、上海泛微网络科技股份有限公司、谷歌公司、金山软件股份有限公司、外语教学与研究出版社有限责任公司、深圳市安居宝电子有限公司、中国建材检验认证集团股份有限公司、北京翰博尔信息技术股份有限公司、厦门科汛软件有限公司、北京金网安泰信息技术有限公司、eml 企业通讯录管理系统、Eview、国微 CMS、飞蛙商城、天睿程序设计公益团队。

本周，CNVD 发布了《关于 Samba 存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4148

本周漏洞报送情况统计

本周，共 19 家成员单位、企业用户及个人用户报送了本周收录的全部 363 个漏洞。报送情况如表 1 所示。其中，蓝盾信息安全技术有限公司、恒安嘉新、启明星辰、安天实验室、天融信等单位报送数量较多。360 网神、漏洞盒子、福建六壬网安股份有限公司、杭州朔方信息技术有限公司、江苏君立华域信息安全技术股份有限公司、中新网络信息安全股份有限公司、清远职业技术学院、安徽新华博信息技术股份有限公司、江西安服信息产业有限公司、广州软云计算机科技有限公司及其他个人白帽子向 CNVD 提交了 561 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
蓝盾信息安全技术有限公司	1459	1
360 网神	281	281
恒安嘉新	246	0
启明星辰	237	14
安天实验室	171	0
漏洞盒子	125	0
天融信	122	0

华为技术有限公司	94	0
H3C	59	0
绿盟科技	39	0
中国电信集团系统集成有限责任公司	37	0
厦门服云信息科技有限公司	31	0
北京数字观星科技有限公司	5	0
广西鑫瀚科技有限公司	5	5
知道创宇	4	4
深圳市深信服电子科技有限公司	3	3
南京铱迅信息技术股份有限公司	1	1
沈阳东软系统集成工程有限公司	1	1
西安四叶草信息技术有限公司	1	1
福建六壬网安股份有限公司	11	11
杭州朔方信息技术有限公司	10	10
江苏君立华域信息安全技术股份有限公司	7	7
中新网络信息安全股份有限公司	5	5
清远职业技术学院	5	5
安徽新华博信息技术股份有限公司	2	2
江西安服信息产业有限公司	2	2
广州软云计算机科技有限公司	1	1
CNCERT 山西分中心	11	11
CNCERT 重庆分中心	8	8

CNCERT 湖南分中心	4	4
CNCERT 北京分中心	2	2
CNCERT 河北分中心	2	2
CNCERT 宁夏分中心	2	2
CNCERT 福建分中心	1	1
CNCERT 新疆分中心	1	1
CNCERT 广东分中心	1	1
个人	175	175
报送总计	3171	561
录入总计	363（去重）	561

表 1 漏洞报送情况统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 363 个漏洞。其中应用程序漏洞 207 个，操作系统漏洞 63 个，web 应用漏洞 46 个，网络设备漏洞 41 个，安全产品漏洞 6 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	207
操作系统漏洞	63
web 应用漏洞	46
网络设备漏洞	41
安全产品漏洞	6

表 2 漏洞按影响类型统计表

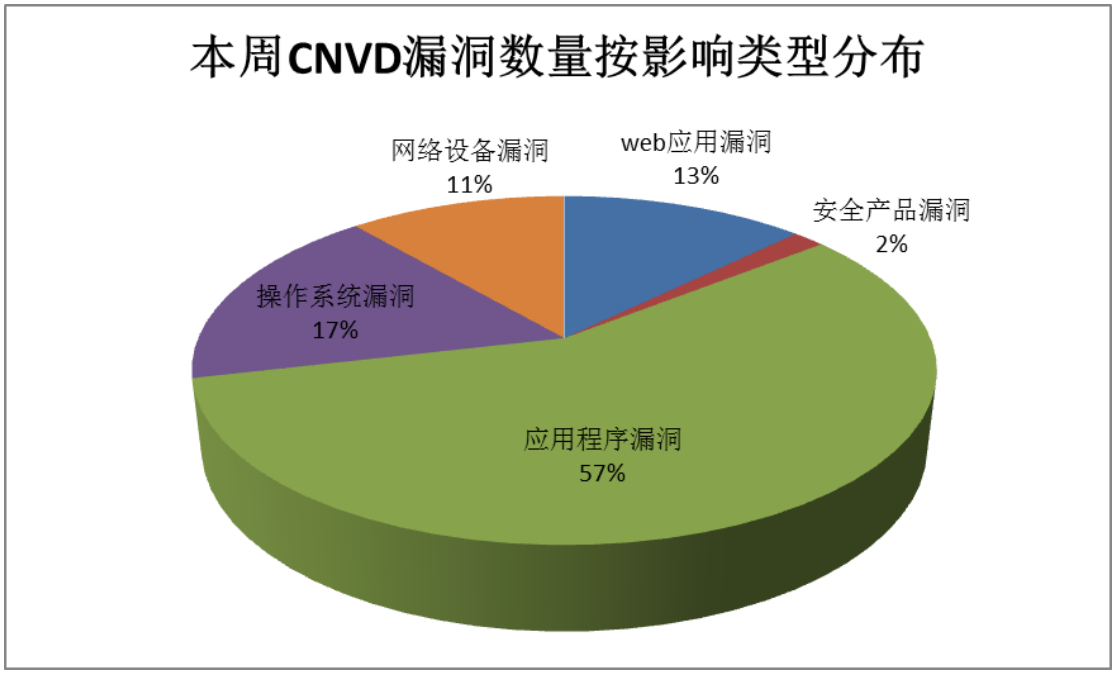

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Cisco、NVIDIA 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	46	13%
2	Cisco	17	5%
3	NVIDIA	15	4%
4	Apple	14	4%
5	Juniper Networks	13	4%
6	Accellion	12	3%
7	GNU	11	3%
8	Microsoft	11	3%
9	IBM	9	2%
10	其他	215	59%

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 24 个电信行业漏洞，44 个移动互联网行业漏洞，3 个工控系统行业漏洞（如下图所示）。其中，“Wecon Technologies LEVI Studio HMI Editor 堆缓冲区溢出漏洞、HP Network Automation SQL 注入漏洞（CNVD-2017-07619）、HP Net

work Automation 远程代码执行漏洞（CNVD-2017-07620）、Samsung SM-G920F SecEmailSync SQL 注入漏洞、D-Link DAP-1360 跨站请求伪造漏洞（CNVD-2017-07250）、IBM Informix Dynamic Server Open Admin Tool 远程代码执行漏洞、Google Android OS HTTP 头注入漏洞、Apple iOS AVEVideoEncoder 内存破坏漏洞”等的综合评级为“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/

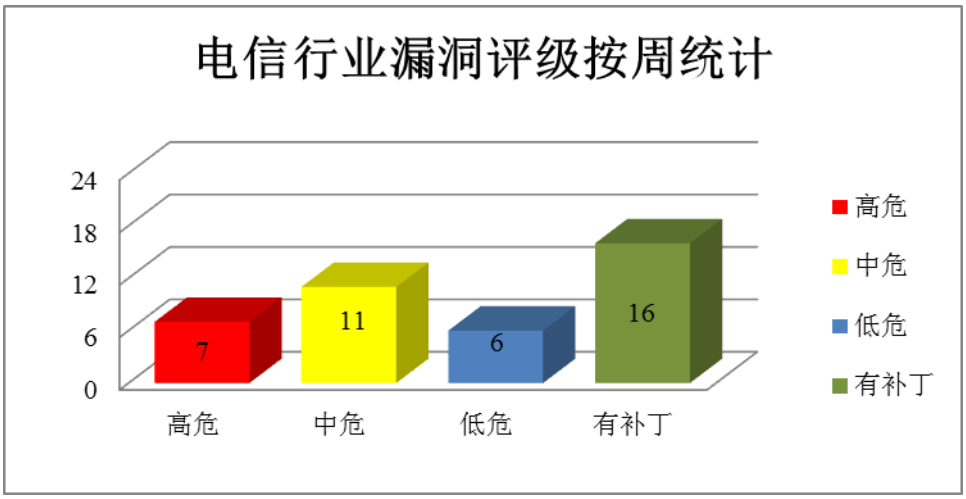

图 3 电信行业漏洞统计

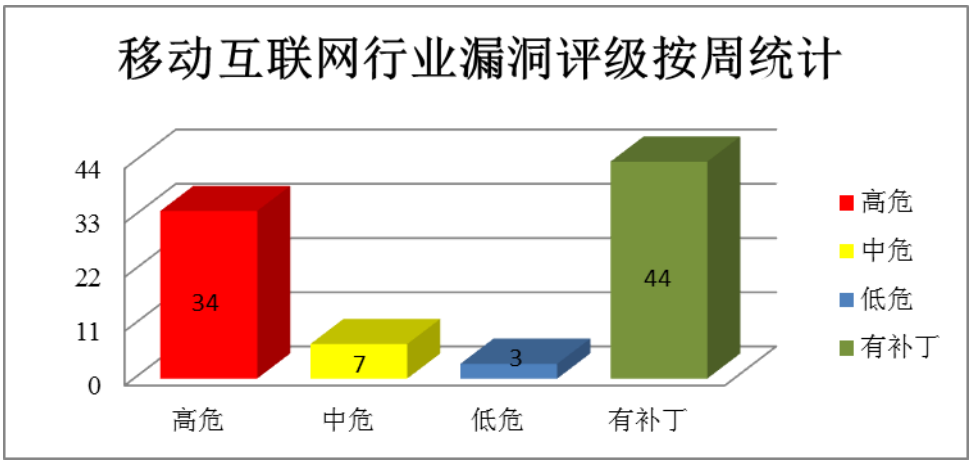

图 4 移动互联网行业漏洞统计

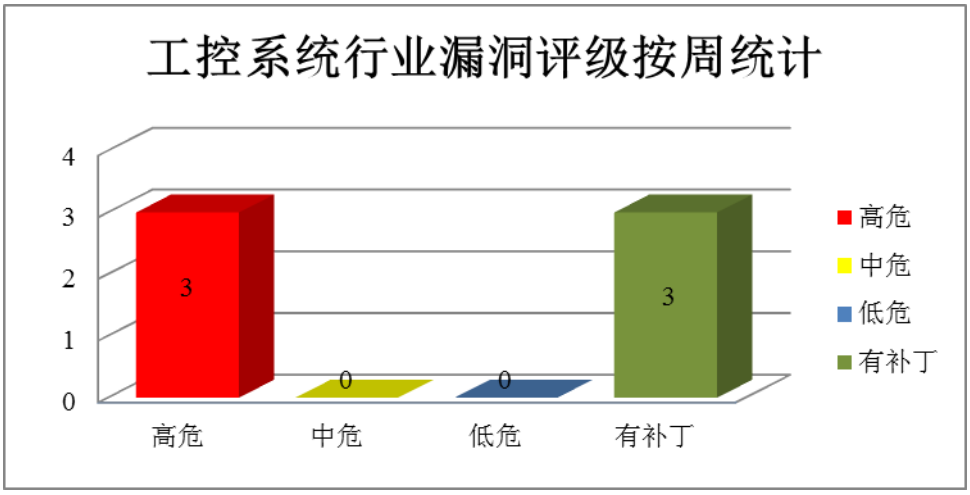

图 5 工控系统行业漏洞统计

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、Samba 服务器软件远程代码执行漏洞

Samba 是运行于 Linux 和 UNIX 系统上实现 SMB 协议的软件。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用客户端将指定库文件上传到具有可写权限的共享目录，使服务器加载并执行指定的库文件，执行任意代码。

CNVD 收录的相关漏洞包括：Samba 服务器软件远程代码执行漏洞。该漏洞的综合评级为“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-2017-07432

2、Google 产品安全漏洞

Google Android 是一款基于 Linux 的应用于智能手机设备的操作系统。本周，该产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android MediaTek Thermal Driver 权限提升漏洞（CNVD-2017-07434、CNVD-2017-07435、CNVD-2017-07436）、Google Android Qualcomm Sound Driver 权限提升漏洞（CNVD-2017-07258、CNVD-2017-07366）、Google Android Qualcomm Video Driver 权限提升漏洞（CNVD-2017-07363、CNVD-2017-07364、CNVD-2017-07365）。上述漏洞的综合评级为“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-2017-07434

http://www.cnvd.org.cn/flaw/show/CNVD-2017-07435

http://www.cnvd.org.cn/flaw/show/CNVD-2017-07436

http://www.cnvd.org.cn/flaw/show/CNVD-2017-07258
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07366
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07363
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07364
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07365

3、Microsoft 产品安全漏洞

Microsoft Chakra 是美国微软（Microsoft）公司的一个 Edge 所使用的 JavaScript 引擎组件。Microsoft ASP.NET Core 是一个跨平台开源框架。Sever Message Block（SMB）是一个为计算机提供身份验证用以访问服务器上打印机和文件系统的组件。Microsoft Office 是一套基于 Windows 操作系统的办公软件套装。本周，上述产品被披露存在远程代码执行、拒绝服务和权限提升漏洞，攻击者可利用漏洞执行任意代码、发起拒绝服务攻击或提升权限。

CNVD 收录的相关漏洞包括：Microsoft ASP.NET Core 拒绝服务漏洞、Microsoft ASP.NET Core 权限提升漏洞、Microsoft Chakra 远程代码执行漏洞、Microsoft Chakra Core 远程代码执行漏洞、Microsoft Office 远程代码执行漏洞（CNVD-2017-07394）、Microsoft Windows SMB Server 远程代码执行漏洞（CNVD-2017-07390、CNVD-2017-07391、CNVD-2017-07392）。除“Microsoft ASP.NET Core 拒绝服务漏洞”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-2017-07322
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07323
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07324
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07393
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07394
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07390
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07391
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07392

4、Apple 产品安全漏洞

Apple iOS 和 Safari 都是美国苹果（Apple）公司的产品。Apple iOS 是为移动设备所开发的一套操作系统，Safari 是一款 Web 浏览器。WebKit 是一套开源 Web 浏览器引擎。AVEVideoEncoder 是的一个视频编码器。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意的代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apple iOS 和 Safari WebKit 内存破坏漏洞（CNVD-2017-07602、CNVD-2017-07603、CNVD-2017-07604、CNVD-2017-07605、CNVD-2017-07606、CNVD-2017-07608、CNVD-2017-07610）、Apple iOS AVEVideoEncoder 内存破

坏漏洞。上述漏洞的综合评级为“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-2017-07602
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07603
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07604
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07605
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07606
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07608
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07610
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07189

5、Cisco Industrial Ethernet 1000 Series Switches 跨站请求伪造漏洞

Cisco Industrial Ethernet 1000 Series Switches 是美国思科（Cisco）公司的工业级以太网 1000 系列交换机。本周，Cisco 被披露存在跨站请求伪造漏洞，攻击者可通过诱使界面的用户打开恶意的链接或访问攻击者控制的网站利用该漏洞实施未授权的操作。目前，互联网上已经出现了针对该漏洞的攻击代码，厂商尚未发布漏洞修补程序。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-2017-07539

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-2017-07132	F5 SSL Intercept iApp 命令执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://support.f5.com/csp/article/K53244431
CNVD-2017-07182	Detcon SiteWatch Gateway 身份验证漏洞	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://www.detcon.com/
CNVD-2017-07208	GNU Binutils 存在未明漏洞	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：https://www.gnu.org/
CNVD-2017-07244	UDFclient 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=861347
CNVD-2017-07249	Tuleap Project Wiki 命令注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：

			https://tuleap.net
CNVD-2017-07250	D-Link DAP-1360 跨站请求伪造漏洞（CNVD-2017-07250）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.dlink.com/
CNVD-2017-07261	多款 GE 产品弱密码漏洞	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：https://www.gegridsolutions.com/
CNVD-2017-07387	EMC RSA Adaptive Authentication 跨站脚本漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.emc.com/
CNVD-2017-07453	Accellion FTA 设备 SQL 注入漏洞	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://www.accellion.com/
CNVD-2017-07452	Accellion FTA 设备 LDAP 注入漏洞	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://www.accellion.com/

表 4 部分重要高危漏洞列表

小结：本周，Samba 被披露存在远程代码执行漏洞，攻击者可利用客户端将指定库文件上传到具有可写权限的共享目录，使服务器加载并执行指定的库文件，执行任意代码。此外，Microsoft 、Google、Apple 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、提升权限或发起拒绝服务攻击等。另外，Cisco 被披露存在跨站请求伪造漏洞，攻击者可通过诱使界面的用户打开恶意的链接或访问攻击者控制的网站利用该漏洞实施未授权的操作。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。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、WordPress Spider Event Calendar SQL 注入漏洞

验证描述

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。Spider Event Calendar 是其中的一个高度可配置的日历插件。

WordPress Spider Event Calendar 插件 1.5.52 之前的版本中存在 SQL 注入漏洞。远程攻击者可通过向 calendar_functions.php 或 widget_Theme_functions.php 文件发送‘order_by’参数利用该漏洞执行任意的 SQL 命令。

验证信息

POC 链接：http://lists.openwall.net/full-disclosure/2017/04/09/1

漏洞链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-07215

信息提供者

恒安嘉新（北京）科技有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. Samba 远程代码执行漏洞

Samba 是 Linux 和 UNIX 系统的 SMB 协议服务软件，可以实现与其他操作系统（如：微软 Windows 操作系统）进行文件系统、打印机和其他资源的共享。此次漏洞最早影响到 7 年前的版本，黑客可以利用漏洞进行远程代码执行。最安全的方法还是打补丁或者升级到 Samba 4.6.4/4.5.10/4.4.14 任意版本。

参考链接：http://www.freebuf.com/vuls/135624.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