

## 信息安全漏洞周报

2016 年 11 月 21 日-2016 年 11 月 27 日

2016 年第 48 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 185 个，其中高危漏洞 60 个、中危漏洞 110 个、低危漏洞 15 个。漏洞平均分为 5.91。本周收录的漏洞中，涉及 0day 漏洞 29 个（占 16%）。其中互联网上出现“WordPress 插件 Answer My Question SQL 注入漏洞、TP-LINK TDDP 缓冲区溢出漏洞”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 602 个，与上周（569 个）环比增长 6%。

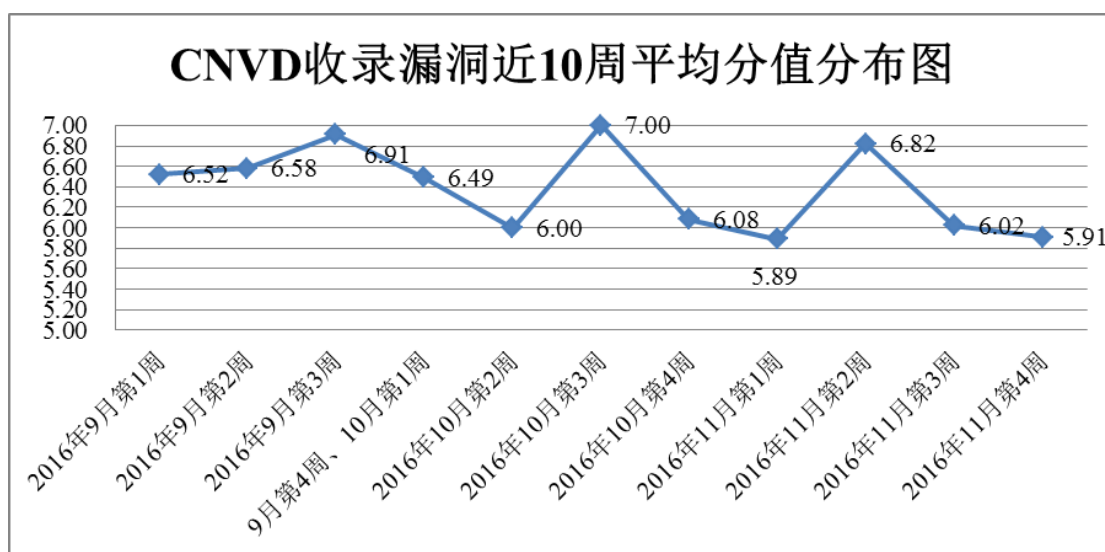


图 1 CNVD 收录漏洞近 10 周平均分分布图

### 本周漏洞报送情况统计

本周，共 6 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 185 个漏洞。报送情况如表 1 所示。其中，恒安嘉新、H3C、北京数字观星科技有限公司、启明星辰等单位报送数量较多。360 网神、漏洞盒子、广西鑫瀚科技有限公司、广州圣

辉信息技术有限公司、南京铨迅信息技术股份有限公司、新疆天山智汇信息科技有限公司、江苏省信息安全测评中心、蚂蚁金服巴斯光年实验室及其他个人白帽子向 CNVD 提交了 602 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 |
|----------------|---------|--------|
| 360 网神         | 485     | 485    |
| 恒安嘉新           | 103     | 1      |
| H3C            | 60      | 0      |
| 北京数字观星科技有限公司   | 7       | 0      |
| 启明星辰           | 0       | 2      |
| 漏洞盒子           | 53      | 53     |
| 广西鑫瀚科技有限公司     | 4       | 4      |
| 广州圣辉信息技术有限公司   | 3       | 3      |
| 南京铨迅信息技术股份有限公司 | 1       | 1      |
| 新疆天山智汇信息科技有限公司 | 1       | 1      |
| 江苏省信息安全测评中心    | 1       | 1      |
| 蚂蚁金服巴斯光年实验室    | 1       | 1      |
| CNCERT 江西分中心   | 8       | 8      |
| CNCERT 宁夏分中心   | 1       | 1      |
| 个人             | 41      | 41     |
| 报送总计           | 769     | 602    |
| 录入总计           | 185（去重） | 602    |

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 185 个漏洞。其中应用程序漏洞 126 个，web 应用漏洞 27 个，

网络设备漏洞 19 个，操作系统漏洞 10 个，安全产品漏洞 3 个。

| 漏洞影响对象类型 | 漏洞数量 |
|----------|------|
| 应用程序漏洞   | 126  |
| web 应用漏洞 | 27   |
| 网络设备漏洞   | 19   |
| 操作系统漏洞   | 10   |
| 安全产品漏洞   | 3    |

表 2 漏洞按影响类型统计表

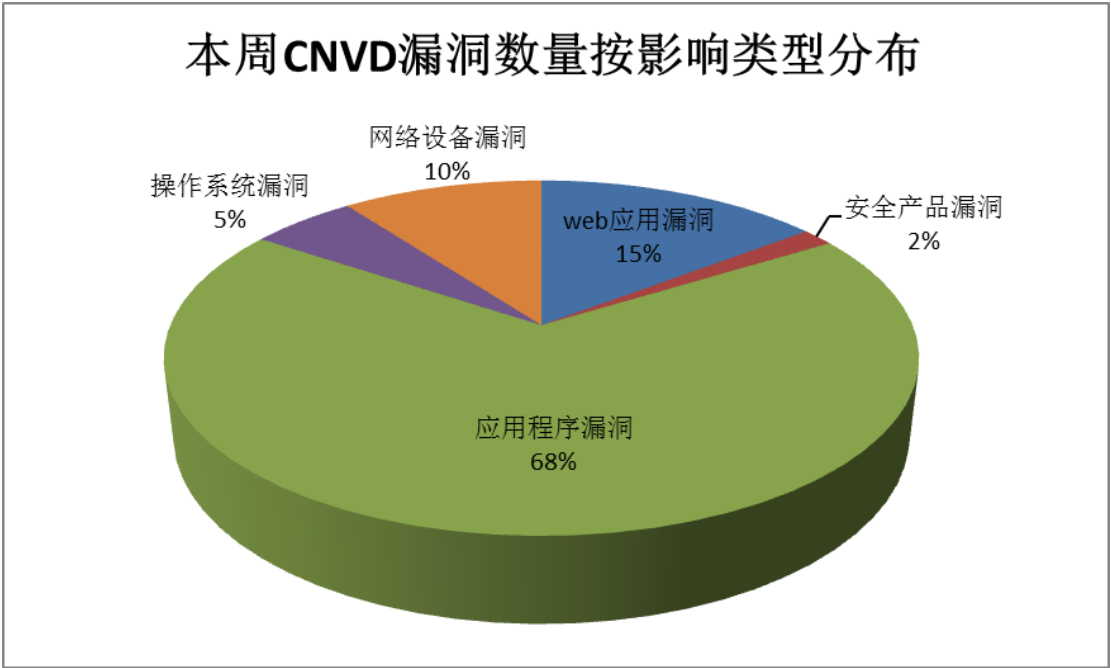


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mozilla、IBM、JasPer 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  | Mozilla                | 30   | 16%  |
| 2  | IBM                    | 13   | 7%   |
| 3  | JasPer                 | 13   | 7%   |
| 4  | NTP                    | 10   | 5%   |
| 5  | Silicon Graphics, Inc. | 7    | 4%   |
| 6  | SIEMENS                | 7    | 4%   |
| 7  | Lepton                 | 6    | 3%   |
| 8  | Linux                  | 4    | 2%   |
| 9  | HDF5                   | 4    | 2%   |
| 10 | 其他                     | 91   | 50%  |

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 4 个电信行业漏洞，3 个移动互联网行业漏洞，6 个工控系统行业漏洞（如下图所示）。其中，“Huawei Flybox B660 Router 绕过验证漏洞、多款 Huawei 产品拒绝服务漏洞（CNVD-2016-11388）、多款 Android 产品中间人安全绕过漏洞、西门子上位机 Profinet Discovery 服务拒绝服务漏洞、Siemens SIMATIC S7-300/1200/1500 CPU 拒绝服务漏洞、Siemens SIMATIC S7-300 CPU 拒绝服务漏洞”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/>

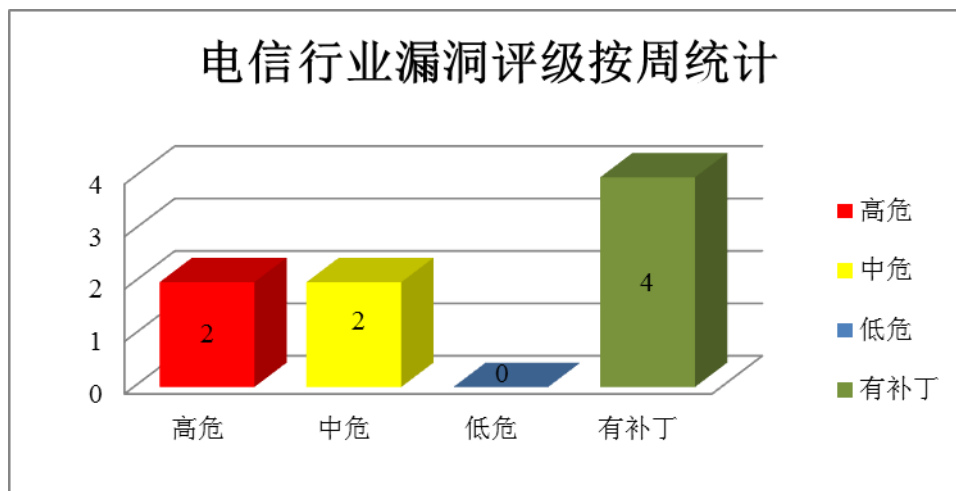


图 3 电信行业漏洞统计

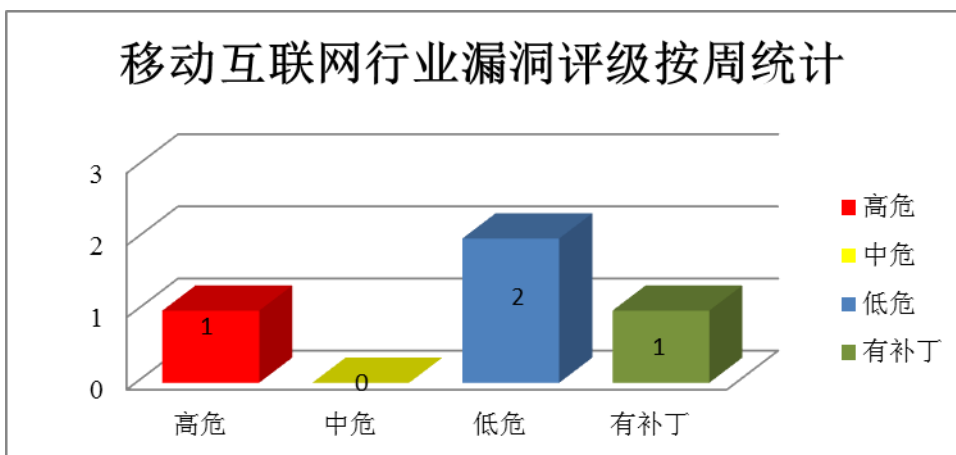


图 4 移动互联网行业漏洞统计

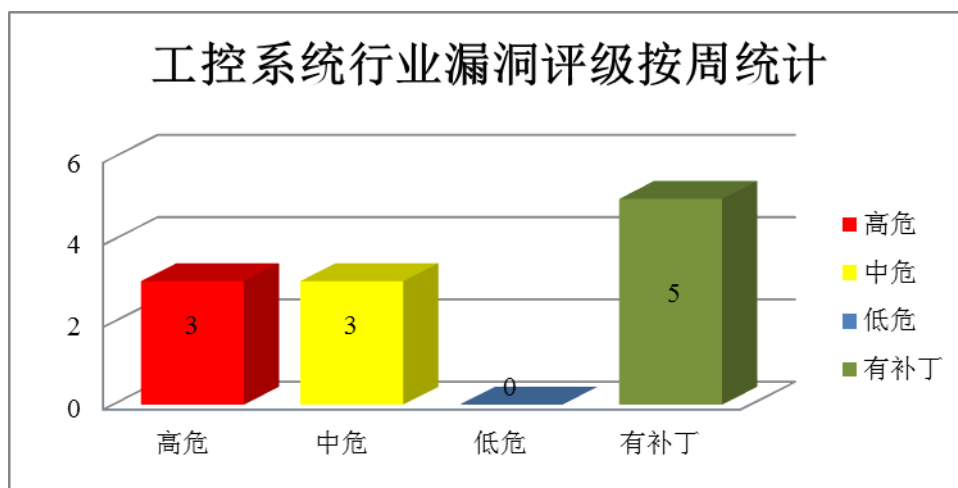


图 5 工控系统行业漏洞统计

## 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、NTP 产品安全漏洞

Network Time Protocol (NTP) 是用于使计算机时间同步化的一种协议，NTPD (Network Time Protocol daemon) 是一个操作系统守护进程。本周，上述产品被披露存在拒绝服务和时间戳绕过漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：ntpd 存在本地拒绝服务漏洞、ntpd 存在拒绝服务高危漏洞、ntpd 零起源时间戳绕过漏洞、ntpd 拒绝服务漏洞 (CNVD-2016-11431、CNVD-2016-11426)、ntpd 广播模式重放防御拒绝服务漏洞、ntpd 存在 NULL 指针引用拒绝服务漏洞、ntpd 广播模式拒绝服务漏洞等。其中，“ntpd 存在拒绝服务高危漏洞”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-2016-11432>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11429>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11430>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11431>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11426>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11423>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11425>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11428>

### 2、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会开发的一款开源 Web 浏览器。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、泄露敏感信息或执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 权限提升漏洞（CNVD-2016-11412）、Mozilla Firefox 内存破坏漏洞（CNVD-2016-11467）、Mozilla Firefox 时序攻击漏洞、Mozilla Firefox 权限提升漏洞、Mozilla Firefox 缓冲区溢出漏洞（CNVD-2016-11480）、Mozilla Firefox 中间人攻击漏洞（CNVD-2016-11481）、Mozilla Firefox 整数溢出漏洞（CNVD-2016-11474）、Mozilla Firefox 任意文件写入漏洞等。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-2016-11412>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11467>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11483>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11413>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11480>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11481>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11474>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11472>

### 3、IBM 产品安全漏洞

IBM Kenexa LCMS Premier on Cloud 是美国 IBM 公司的一套可调节的用于开发、维护和提供高效的员工培训的学习内容管理系统（LCMS）。IBM Connections 是美国 IBM 公司一套社交软件平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息或发起跨站脚本攻击等。

CNVD 收录的相关漏洞包括：IBM Connections 跨站请求伪造漏洞（CNVD-2016-11313、CNVD-2016-11315）、IBM Connections 信息泄露漏洞（CNVD-2016-11314、CNVD-2016-11316）、IBM Kenexa LCMS Premier on Cloud 跨站脚本漏洞、IBM Kenexa LCMS Premier on Cloud 跨站脚本漏洞（CNVD-2016-11444）、IBM Kenexa LCMS Premier on Cloud 跨站请求伪造漏洞、IBM Kenexa LCMS Premier on Cloud 信息泄露漏洞等。其中，“IBM Kenexa LCMS Premier on Cloud 跨站请求伪造漏洞、IBM Kenexa LCMS Premier on Cloud 信息泄露漏洞”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-2016-11313>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11315>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11314>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11316>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11442>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11444>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11441>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11443>

#### 4、JasPer 产品安全漏洞

JasPer 是一个 JPEG-2000 编解码器的开源实现。本周，该产品被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：JasPer 拒绝服务漏洞（CNVD-2016-11390、CNVD-2016-11391、CNVD-2016-11395、CNVD-2016-11396、CNVD-2016-11397、CNVD-2016-11398、CNVD-2016-11399、CNVD-2016-11400）等。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-2016-11390>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11391>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11395>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11396>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11397>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11398>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11399>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11400>

#### 5、Google Pixel 远程代码执行漏洞

Google Pixel 是美国谷歌（Google）公司的一款平板电脑。本周，Google 被披露存在远程代码执行漏洞。攻击者可利用该漏洞执行任意代码。目前，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-2016-11450>

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-2016-11307 | BigTree CMS SQL 注入漏洞        | 高    | 用户可联系供应商获得补丁信息：<br><a href="https://www.bigtreecms.org/">https://www.bigtreecms.org/</a> |
| CNVD-2016-11317 | pycsw 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，补丁获取链接：<br><a href="http://pycsw.org/">http://pycsw.org/</a>       |
| CNVD-2016-11357 | Moxa SoftCMS SQL 注入漏洞       | 高    | 厂商已提供漏洞修补方案，请关注厂商主页及时更新：<br><a href="http://www.moxa.com">http://www.moxa.com</a>        |
| CNVD-2016-11356 | Moxa SoftCMS 拒绝服务漏洞         | 高    | 厂商已提供漏洞修补方案，请关注厂商主页及时更新：<br><a href="http://www.moxa.com">http://www.moxa.com</a>        |
| CNVD-201        | Teeworlds 'client.cpp'内存破坏漏 | 高    | 用户可联系供应商获得补丁信息：                                                                          |

|                 |                                  |   |                                                                                                                         |
|-----------------|----------------------------------|---|-------------------------------------------------------------------------------------------------------------------------|
| 6-11439         | 洞                                |   | <a href="http://www.ece.uvic.ca/">http://www.ece.uvic.ca/</a>                                                           |
| CNVD-2016-11458 | Barco ClickShare 远程代码执行漏洞        | 高 | 用户可联系供应商获得补丁信息：<br><a href="http://www.barco.com.cn/zh-CN/clickshare">http://www.barco.com.cn/zh-CN/clickshare</a>      |
| CNVD-2016-11477 | HDF5 代码执行漏洞<br>(CNVD-2016-11477) | 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：<br><a href="https://support.hdfgroup.org/HDF5/">https://support.hdfgroup.org/HDF5/</a> |
| CNVD-2016-11476 | HDF5 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：<br><a href="https://support.hdfgroup.org/HDF5/">https://support.hdfgroup.org/HDF5/</a> |
| CNVD-2016-11475 | HDF5 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：<br><a href="https://support.hdfgroup.org/HDF5/">https://support.hdfgroup.org/HDF5/</a> |
| CNVD-2016-11478 | HDF5 堆缓冲区溢出漏洞                    | 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：<br><a href="https://support.hdfgroup.org/HDF5/">https://support.hdfgroup.org/HDF5/</a> |

表 4 部分重要高危漏洞列表

小结：本周，NTP 产品被披露存在拒绝服务和时间戳绕过漏洞，攻击者可利用漏洞发起拒绝服务攻击。此外，Mozilla、IBM、JasPer 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、提升权限、执行任意代码和发起跨站脚本攻击等。另外，Google 被披露存在远程代码执行漏洞。攻击者可利用该漏洞执行任意代码。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. 利用 SQLite 数据库文件实现任意代码执行

近期，我们对贝尔金 WeMo 智能家居设备的安全性进行了分析。在研究过程中，我们开发出了一种新型的 SQL 注入技术，这项技术针对的是 SQLite 数据库。实验表明，我们可以利用这项 SQLite 注入技术在 SQLite 数据库中实现任意代码执行。攻击者就可以使用恶意 PHP 代码来对该文件进行处理，当攻击者向服务器请求该文件时，PHP 解释器就会执行其中的恶意代码。

参考链接：<http://www.freebuf.com/vuls/120213.html>

### 2. WordPress 自动更新机制的严重漏洞

Wordfence 最近披露了某个影响范围很广的安全问题，大量 WordPress 网站都受到影响。攻击者通过 [api.wordpress.org](http://api.wordpress.org) 的自动更新机制，就能大规模黑入大量 WordPress 站点。Wordfence 宣称，整个 web 世界有 27% 的网站都可能因此被黑。简单说就是利用

WordPress 更新服务器的弱点，控制该服务器，自然也就能够同时对所有采用 WordPress 的网站完成入侵了。Wordfence 表示 api.wordpress.org 仍然是部署 WordPress 核心、插件和主题升级的单点故障根源所在。

参考链接: <http://www.freebuf.com/vuls/121018.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](http://www.cert.org.cn)

邮箱: [vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话: 010-82990999