# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

2016 年 07 月 04 日-2016 年 07 月 10 日　　2016 年第 28 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 101 个，其中高危漏洞 27 个、中危漏洞 59 个、低危漏洞 15 个。漏洞平均分值为 5.51 分。本周收录的漏洞中，涉及 0day 漏洞 10 个（占 10%）。其中互联网上出现“Ktools Photostore SQL 注入漏洞”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 457 个，与上周（518 个）环比下降 12%。

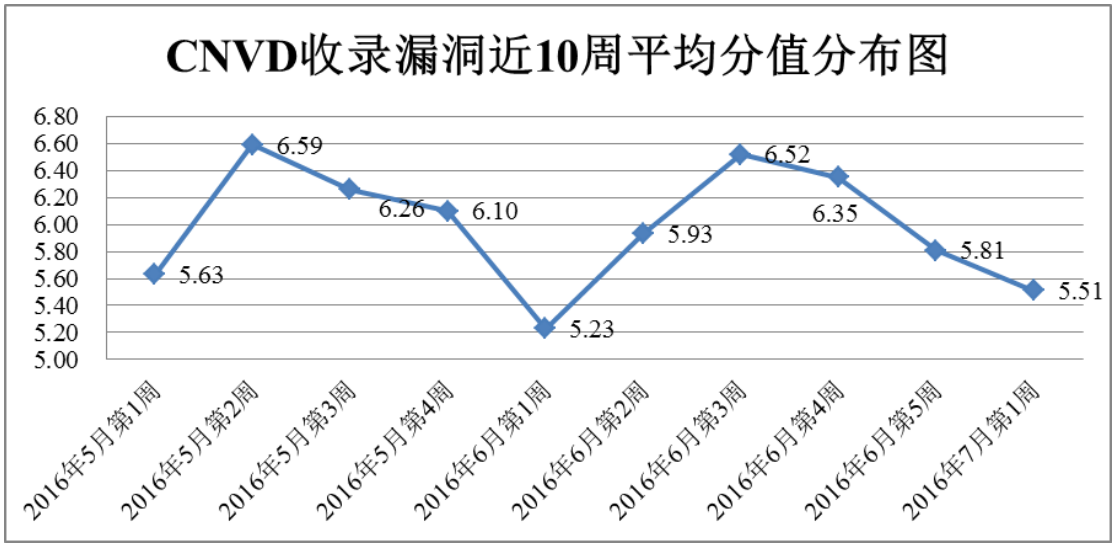


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 本周漏洞报送情况统计

本周，共 8 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 101 个漏洞。报送情况如表 1 所示。其中，东软、绿盟科技、天融信、启明星辰等单位报送数量较多。补天平台、乌云、漏洞盒子、深圳市深信服电子科技有限公司、西安四叶草信息技术有限公司及其他个人白帽子向 CNVD 提交了 457 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 |
|---|---|---|
| 东软 | 203 | 0 |
| 绿盟科技 | 158 | 0 |
| 天融信 | 90 | 0 |
| 启明星辰 | 90 | 2 |
| 安天实验室 | 79 | 0 |
| 恒安嘉新 | 61 | 7 |
| 中国电信集团系统集成有限责任公司 | 58 | 0 |
| H3C | 8 | 0 |
| 乌云 | 380 | 380 |
| 漏洞盒子 | 29 | 29 |
| 深圳市深信服电子科技有限公司 | 20 | 20 |
| 西安四叶草信息技术有限公司 | 1 | 1 |
| CNCERT 江西分中心 | 2 | 2 |
| 个人 | 16 | 16 |
| 报送总计 | 1195 | 457 |
| 录入总计 | 101（去重） | 457 |

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 101 个漏洞。其中应用程序漏洞 60 个，网络设备漏洞 13 个，安全产品漏洞 12 个，web 应用漏洞 8 个，操作系统漏洞 7 个，数据库漏洞 1 个。

| 漏洞影响对象类型 | 漏洞数量 |
|---|---|
| 应用程序漏洞 | 60 |
| 网络设备漏洞 | 13 |

| | |
|---|---|
| 安全产品漏洞 | 12 |
| Web 应用漏洞 | 8 |
| 操作系统漏洞 | 7 |
| 数据库漏洞 | 1 |

表 2 漏洞按影响类型统计表

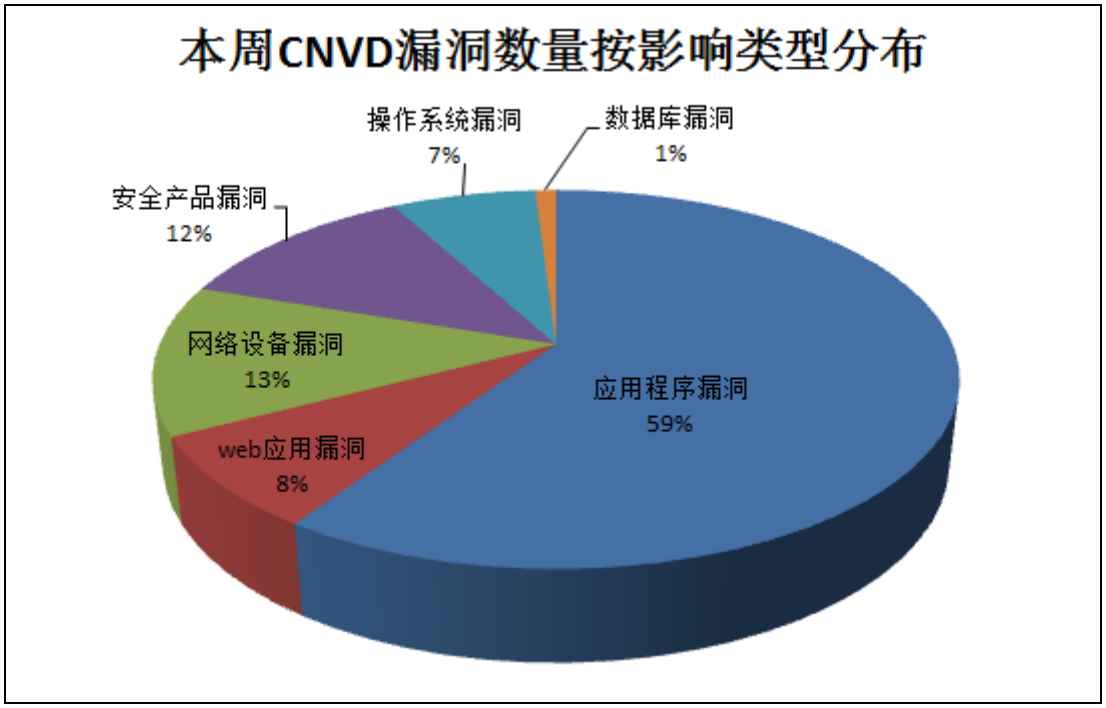


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Cisco、Symantec、IBM 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 | Cisco | 11 | 11% |
| 2 | Symantec | 11 | 11% |
| 3 | IBM | 10 | 10% |
| 4 | Huawei | 9 | 9% |
| 5 | phpMyAdmin | 5 | 5% |
| 6 | Linux | 5 | 5% |
| 7 | Sierra Wireless | 3 | 3% |
| 8 | Lenovo | 3 | 3% |
| 9 | Google | 2 | 2% |
| 10 | 其他 | 42 | 41% |

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 9 个电信行业漏洞，3 个移动互联网行业漏洞，2 个工控系统行业漏洞（如下图所示）。详情请参照 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/

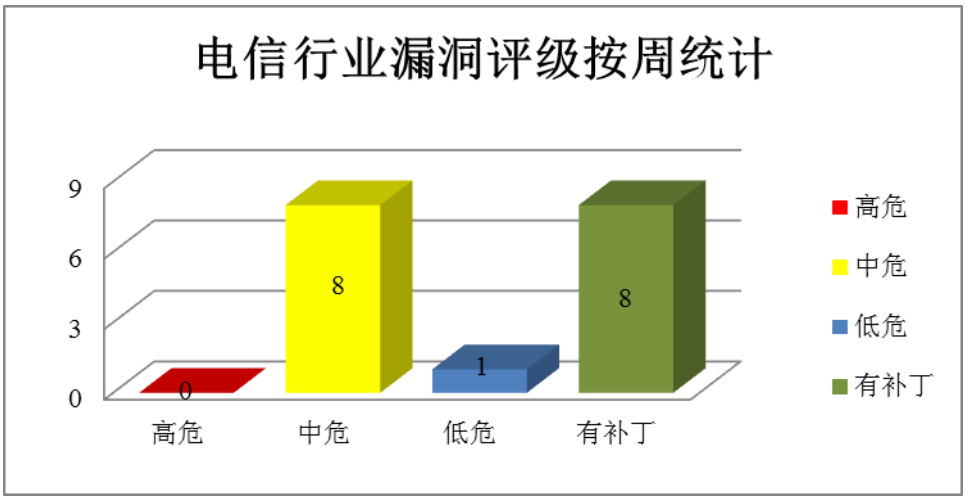


图 3 电信行业漏洞统计

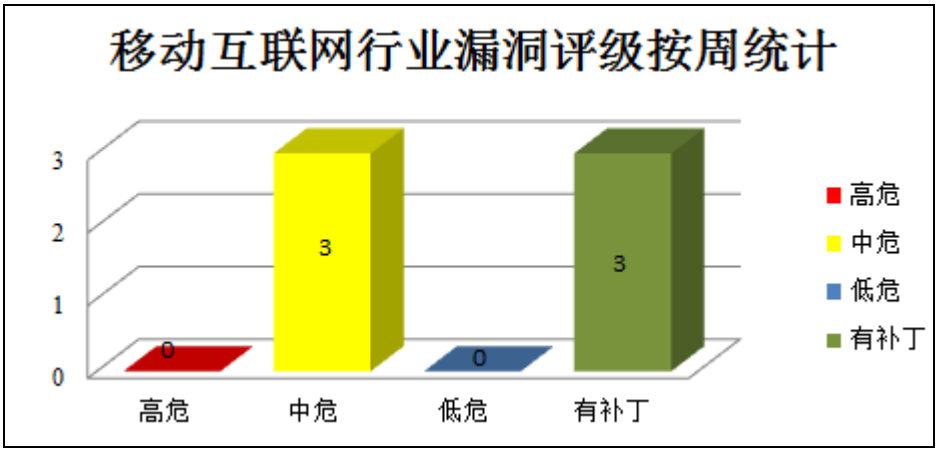


图 4 移动互联网行业漏洞统计

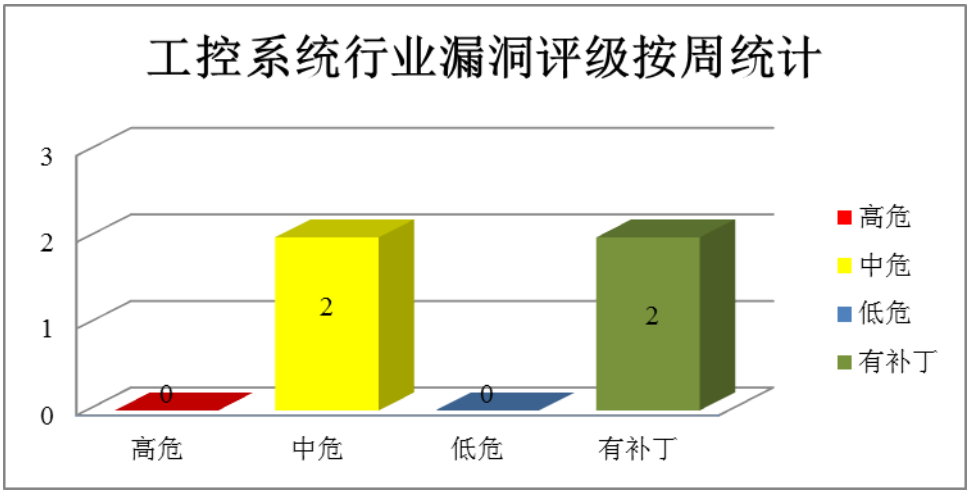


图 5 工控系统行业漏洞统计

## 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、Cisco 产品安全漏洞

Cisco AMP Threat Grid 是美国思科（Cisco）公司的一套集成了静态和动态恶意软件分析以及威胁情报于一体的解决方案；Cisco Prime Infrastructure（PI）是一套通过 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 Expressway 和 Cisco TelePresence Video Communication Server（VCS）都是网真视频通信服务器；Cisco EPC3928 是一款无线路由器产品；Cisco Configuration Assistant（CCA）是一套用于简化配置、部署和管理思科智能商业通信系统的解决方案。Cisco Cloud Network Automation Provisioner（CNAP）是其中的一套云网络自动化配置软件；Cisco Firepower System Software 是一款下一代防火墙产品（NGFW）。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取权限、执行未授权操作和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco AMP Threat Grid 未授权访问漏洞、Cisco Prime Infrastructure HTML 注入漏洞、Cisco Video Communication Server 和 Expressway 身份绕过漏洞、Cisco EPC3928 拒绝服务漏洞（CNVD-2016-04559）、Cisco EPC3928 信息泄露漏洞、Cisco EPC3928 拒绝服务漏洞、Cisco Configuration Assistant Cloud Network Automation Provisioner 信息泄露漏洞、Cisco Firepower System Software 权限获取漏洞等。其中，“Cisco Firepower System Software 权限获取漏洞”的综合评级为“高危”。目前，厂商已经发布了除“Cisco Prime Infrastructure HTML 注入漏洞、Cisco Configuration Assistant Cloud Network Automation Provisioner 信息泄露漏洞”外其余漏洞的修补程序。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-2016-04615

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04616
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04617
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04559
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04560
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04561
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04456
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04455

**2、Symantec 产品安全漏洞**

Symantec Endpoint Protection Manager（SEPM）是美国赛门铁克（Symantec）公司的一套企业级病毒防护软件，Symantec Advanced Threat Protection（ATP）、Symantec Embedded Security:Critical System Protection（SES:CSP）和 Symantec Data Center Security: Server Advanced（SDCS:SA）都是美国赛门铁克（Symantec）公司的安全产品。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞绕过安全限制、执行任意代码和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Symantec Endpoint Protection Manager 权限绕过漏洞、多款 Symantec 和 Norton 产品整数溢出漏洞、多款 Symantec 和 Norton 产品内存破坏漏洞（CNVD-2016-04441、CNVD-2016-04439、CNVD-2016-04437）、多款 Symantec 和 Norton 产品缓冲区溢出漏洞（CNVD-2016-04440）、多款 Symantec 和 Norton 产品缓冲区溢出漏洞、多款 Symantec 和 Norton 产品内存破坏漏洞等。其中，除“多款 Symantec 和 Norton 产品整数溢出漏洞”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-2016-04463
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04442
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04441
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04439
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04437
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04440
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04438
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04436

**3、IBM 产品安全漏洞**

IBM WebSphere Application Server（WAS）是美国 IBM 公司开发并发行的一款应用服务器产品；IBM Hardware Management Console（HMC）是一套用于配置和管理 Power System 系列服务器的图形界面软件；IBM Watson 是一套技术平台；IBM Cognos Business Intelligence（BI）是一套商业智能软件；IBM WebSphere Commerce 是一套电

子商务解决方案；IBM Tivoli Storage Manager（TSM）是一套备份和恢复管理解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、进行跨站脚本攻击和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server Liberty Profile 信息泄露漏洞、IBM Hardware Management Console 权限提升漏洞、IBM Watson Developer Cloud 弱口令漏洞、IBM Cognos Business Intelligence Cognos TM1 跨站脚本漏洞、IBM Cognos Business Intelligence 跨站脚本漏洞、IBM WebSphere Commerce 跨站请求伪造漏洞（CNVD-2016-04564、CNVD-2016-04472）、IBM Tivoli Storage Manager 敏感信息泄露漏洞等。其中，“IBM Hardware Management Console 权限提升漏洞”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-2016-04552
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04551
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04570
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04562
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04563
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04564
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04472
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04459

### 4、Huawei 产品安全漏洞

Huawei Public Cloud Solution 是中国华为（Huawei）公司的一套公有云解决方案；Huawei HiSuite 是一套用于 PC 端的手机助手软件；Huawei AR3200 是一款 AR3200 系列企业路由器产品；Huawei Mate 8 是一款智能手机产品；Huawei FusionCompute 是一套基于 Xen 开源设计的企业级开放式服务器虚拟化解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码、绕过安全限制和实施跨站脚本攻击等。

CNVD 收录的相关漏洞包括：Huawei Public Cloud Solution 跨站脚本漏洞、Huawei HiSuite 任意安装漏洞、Huawei AR3200 MPLS 内存泄露漏洞、Huawei Mate 8 缓冲区溢出漏洞（CNVD-2016-04480）、Huawei Mate 8 安全绕过数据删除漏洞、Huawei FusionCompute 拒绝服务漏洞、Huawei Mate 8 安全绕过漏洞、Huawei HiSuite 任意代码执行漏洞等。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-2016-04555
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04481
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04482

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04480

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04470

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04478

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04479

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04444

### 5、Linux kernel 内存破坏漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，Linux 被披露存在内存破坏漏洞。允许攻击者利用漏洞导致内核崩溃。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-2016-04596

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-2016-04448 | ALSA 'snd_compr_allocate_buffer'函数整数溢出漏洞 | 高 | 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=b35cc8225845112a616e3a2266d2fde5ab13d3ab |
| CNVD-2016-04450 | LibreOffice RTF 解析器内存错误引用漏洞 | 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://www.libreoffice.org/download/libreoffice-fresh/ |
| CNVD-2016-04464 | Opera Mail 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，补丁获取链接：http://www.opera.com/blogs/security/2016/02/opera-12-and-opera-mail-security-update/ |
| CNVD-2016-04466 | Lenovo Solution Center 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，补丁获取链接：https://support.lenovo.com/us/zh/product_security/len_7814 |
| CNVD-2016-04473 | pecl_http 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，补丁获取链接：https://pecl.php.net/package/pecl_http/3.0.1 |
| CNVD-2016-04474 | Silicon Graphics LibTiff 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：http://www.libtiff.org/ |

| | | | |
|---|---|---|---|
| CNVD-2016-04475 | Apache xerces-c 栈缓冲区溢出漏洞 | 高 | 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://svn.apache.org/viewvc?view=revision&revision=1747619 |
| CNVD-2016-04476 | Eaton ELCSoft Programming Software 堆缓冲区溢出漏洞 | 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://www.eaton.com/ |
| CNVD-2016-04483 | Eaton ELCSoft Programming Software 栈缓冲区溢出漏洞 | 高 | 用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.eaton.com/ |
| CNVD-2016-04554 | phpMyAdmin 注入攻击漏洞 | 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://www.phpmyadmin.net/security/PMASA-2016-18/ |

表 4 部分重要高危漏洞列表

小结：本周，Cisco 产品被披露存在多个漏洞，攻击者可利用漏洞获取权限、执行未授权操作和发起拒绝服务攻击等。此外，Symantec、IBM、Huawei 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞获得敏感信息、执行任意代码、进行未授权操作或发起拒绝服务攻击等。另外，Linux 被披露存在内存破坏漏洞。允许攻击者利用漏洞导致内核崩溃。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. 漏洞预警：Spring Boot 框架表达式注入漏洞

Spring 是 2003 年兴起的轻量级 Java 开发框架，Spring Boot 能够大大提升使用 Spring 框架时的开发效率。本周，Spring Boot 框架的 SpEL 表达式注入通用漏洞曝光，利用该漏洞，远程攻击者在服务器上可执行任意命令——该漏洞影响 Spring Boot 版本从 1.1-1.3.0，建议在使用存在此缺陷版本 Spring Boot 的企业立即将之升级至 1.3.1 或以上版本。

参考链接：http://www.freebuf.com/news/108665.html

### 2. 英国国防部在线网关存在漏洞，军队内部数据面临泄露威胁

英国政府安全项目 Government-lab 研究人员 Mohammed Adel 发现了英国国防部在线网关的一个漏洞，Mohammed Adel 使用了一种过滤旁路攻击方式（Filtering Bypass attack）验证了漏洞的存在，这种攻击不需使用@mod.uk 认证的电子邮件就可实现入侵英国国防部网关系统。由于该网关系统仅限国防部内部雇员使用，此漏洞造成的影响可能会使攻击者以内部人员身份入侵系统获取内部信息。

参考链接：http://www.freebuf.com/news/108433.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