# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2017 年 09 月 25 日-2017 年 10 月 08 日** **2017 年第 40、41 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 328 个，其中高危漏洞 119 个、中危漏洞 184 个、低危漏洞 25 个。漏洞平均分值为 6.10。本周收录的漏洞中，涉及 0day 漏洞 60 个（占 18%），其中互联网上出现“ZTE Datacard MF190 权限提升漏洞”零日代码攻击漏洞。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 2028 个。

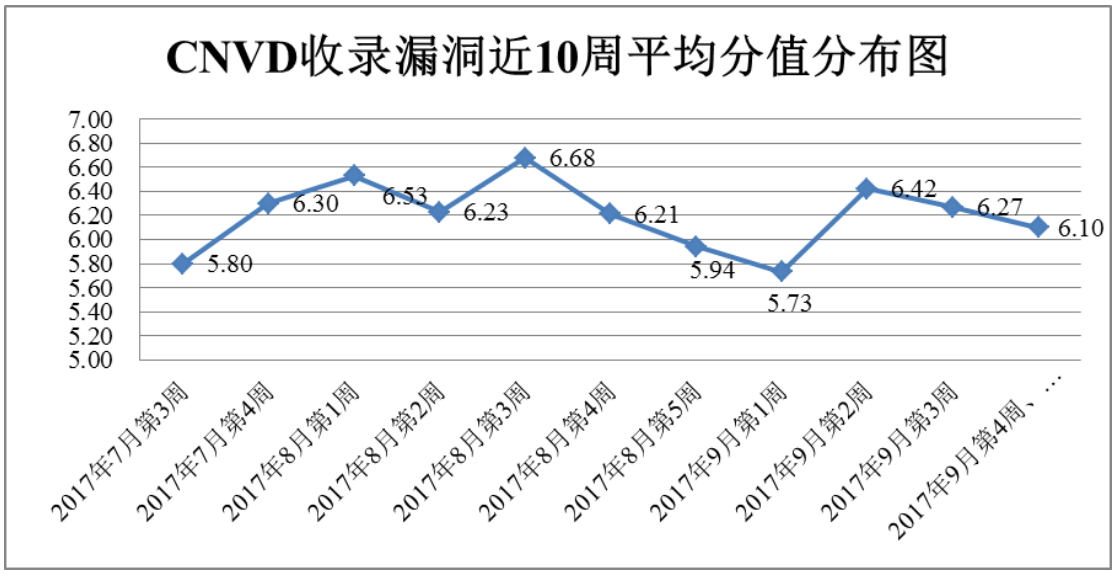


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 本周漏洞报送情况统计

本周，共 14 家成员单位、企业用户及个人用户报送了本周收录的全部 328 个漏洞。报送情况如表 1 所示。其中，华为技术有限公司、安天实验室、恒安嘉新、启明星辰、天融信等单位报送数量较多。四川虹微技术有限公司（子午攻防实验室）、中新网络信息安全股份有限公司、江苏同袍信息科技有限公司、华讯方舟通信设备有限公司、广州

软云计算机科技有限公司、山石网科通信技术有限公司、北京智游网安科技有限公司、北京安码科技有限公司、江苏金盾检测技术有限公司及其他个人白帽子向 CNVD 提交了 2028 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 | 554 | 552 |
| 华为技术有限公司 | 345 | 3 |
| 安天实验室 | 241 | 0 |
| 恒安嘉新 | 189 | 0 |
| 启明星辰 | 182 | 24 |
| 天融信 | 99 | 1 |
| H3C | 83 | 0 |
| 漏洞盒子 | 57 | 57 |
| 杭州安恒信息技术有限公司 | 54 | 0 |
| 中国电信集团系统集成有限责任公司 | 49 | 8 |
| 绿盟科技 | 50 | 0 |
| 厦门服云信息科技有限公司 | 18 | 1 |
| 南京铱迅信息技术股份有限公司 | 1 | 1 |
| 北京无声信息技术有限公司 | 1 | 0 |
| 四川虹微技术有限公司（子午攻防实验室） | 38 | 38 |
| 中新网络信息安全股份有限公司 | 23 | 23 |
| 江苏同袍信息科技有限公司 | 7 | 7 |
| 华讯方舟通信设备有限公司 | 4 | 4 |
| 广州软云计算机科技有限公司 | 2 | 2 |
| 山石网科通信技术有限公司 | 1 | 1 |

| | | |
|---|---|---|
| 北京智游网安科技有限公司 | 1 | 1 |
| 北京安码科技有限公司 | 1 | 1 |
| 江苏金盾检测技术有限公司 | 1 | 1 |
| CNCERT 山西分中心 | 11 | 11 |
| CNCERT 上海分中心 | 7 | 7 |
| CNCERT 吉林分中心 | 6 | 6 |
| CNCERT 天津分中心 | 2 | 2 |
| CNCERT 浙江分中心 | 1 | 1 |
| CNCERT 福建分中心 | 1 | 1 |
| 个人 | 1275 | 1275 |
| 报送总计 | 3304 | 2028 |
| 录入总计 | 328（去重） | 2028 |

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 328 个漏洞。其中应用程序漏洞 241 个，web 应用漏洞 35 个，网络设备漏洞 23 个，操作系统漏洞 19 个，安全产品漏洞 9 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 | 241 |
| web 应用漏洞 | 35 |
| 网络设备漏洞 | 23 |
| 操作系统漏洞 | 19 |
| 安全产品漏洞 | 9 |
| 数据库漏洞 | 1 |

表 2 漏洞按影响类型统计表

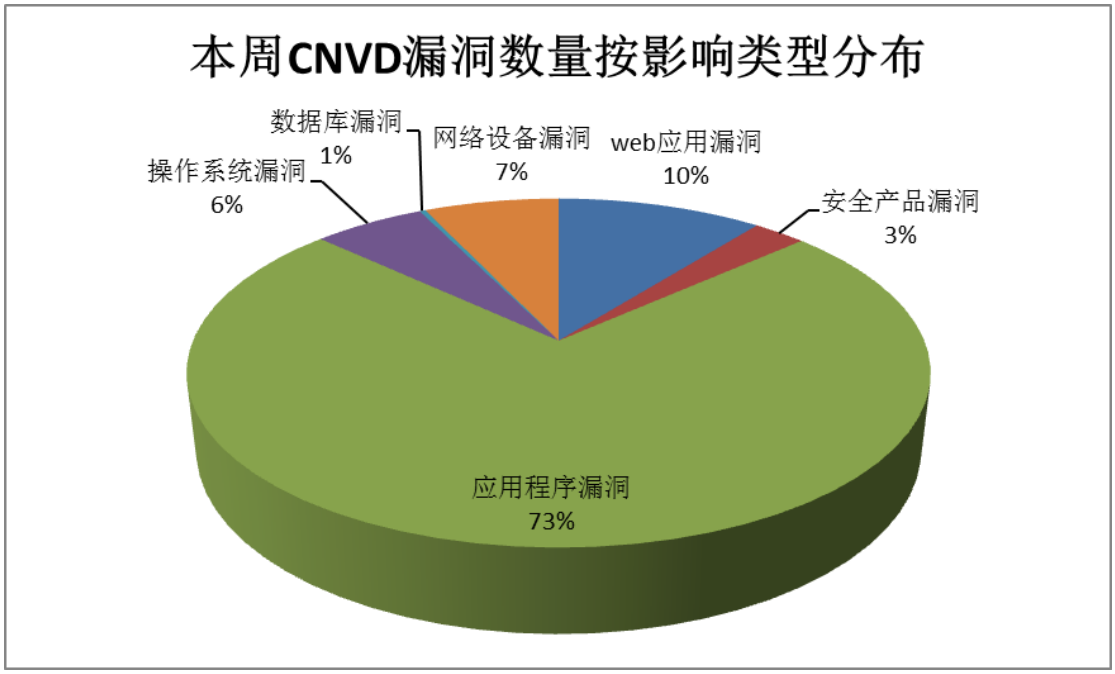


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Tcpdump、Microsoft、Oracle 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 | Tcpdump | 45 | 14% |
| 2 | Microsoft | 36 | 11% |
| 3 | Oracle | 31 | 9% |
| 4 | Adobe | 11 | 3% |
| 5 | Cisco | 8 | 2% |
| 6 | Huawei | 8 | 2% |
| 7 | Apache | 8 | 2% |
| 8 | Red Hat | 7 | 2% |
| 9 | WordPress | 5 | 2% |
| 10 | 其他 | 169 | 53% |

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 个电信行业漏洞，29 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图所示）。其中，“Siemens Ruggedcom ROS and SCALANCE 未授权操作漏洞、Google Android Qualcomm 组件文件系统输入验证漏洞、Apple iOS 缓冲区溢

出漏洞、Huawei 手机写任意内存漏洞”等漏洞的综合评级为“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/

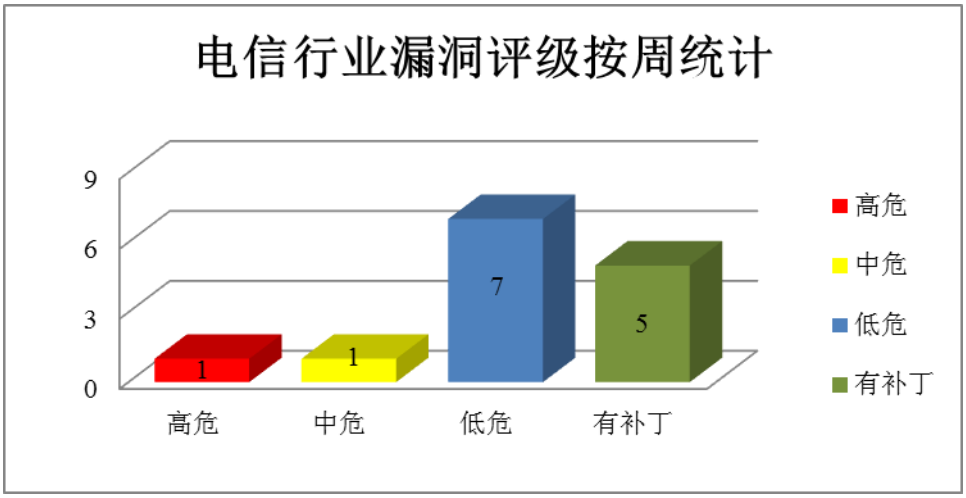


图 3 电信行业漏洞统计

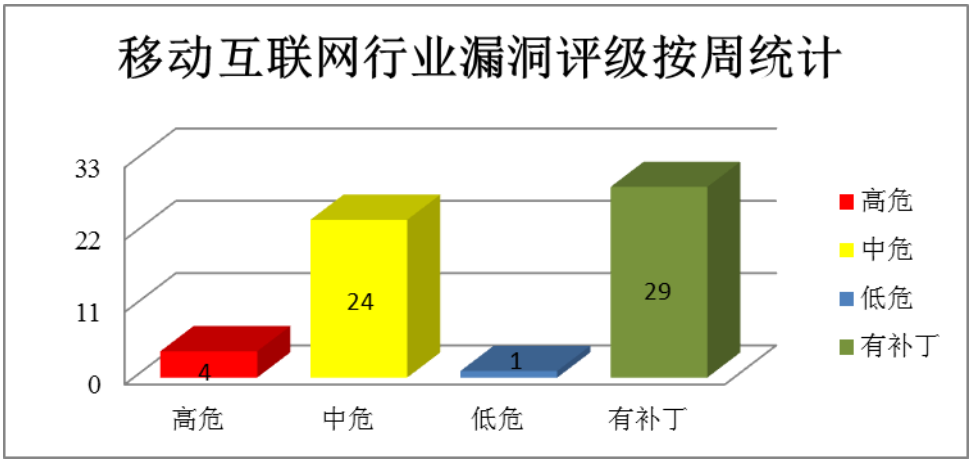


图 4 移动互联网行业漏洞统计

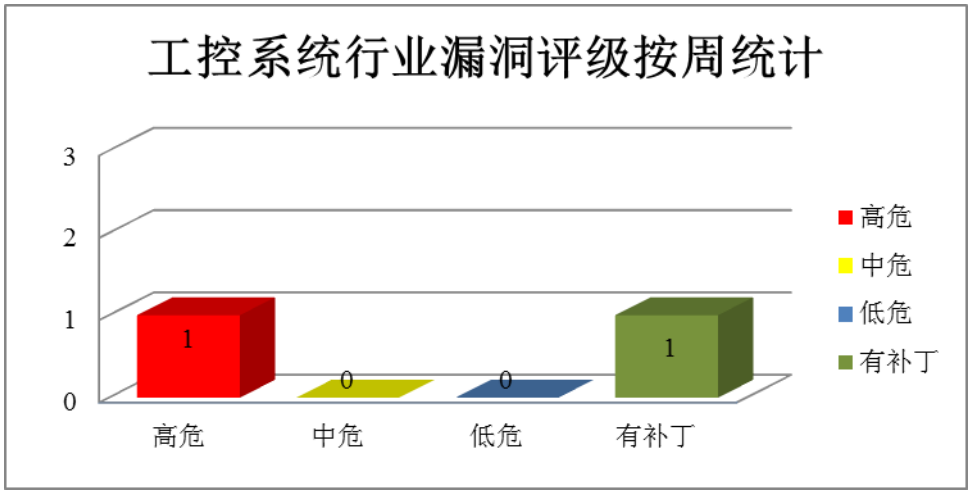

图 5 工控系统行业漏洞统计

## 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、Microsoft 产品安全漏洞

Microsoft Windows 10 是美国微软（Microsoft）公司发布的一套操作系统。Microsoft Edge 是其中的一款系统附带的 Web 浏览器。本周，该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代码。

CNVD 收录的相关漏洞包括：Microsoft Edge 内存破坏漏洞（CNVD-2017-28323、CNVD-2017-28324、CNVD-2017-28646、CNVD-2017-28647、CNVD-2017-28650、CNVD-2017-28651、CNVD-2017-28652、CNVD-2017-28654）。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-2017-28323
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28324
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28646
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28647
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28650
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28651
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28652
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28654

### 2、Tcpdump 产品安全漏洞

Tcpdump 是 Tcpdump 团队开发的一套运行在命令行下的嗅探工具。BGP parser 是其中的一个边界网关协议解析器。IPv6 mobility parser 是其中的一个 IPv6 mobility 解析器。ISO IS-IS parser 是其中的一个路由协议解析器。本周，该产品被披露存在堆缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Tcpdump BGP 解析器缓冲区溢出漏洞（CNVD-2017-28240、CNVD-2017-28247、CNVD-2017-28250）、Tcpdump IPv6 mobility 解析器缓冲区溢出漏洞（CNVD-2017-28284、CNVD-2017-28285）、Tcpdump ISO IS-IS 解析器缓冲区溢出漏洞、Tcpdump ISO IS-IS 解析器缓冲区溢出漏洞（CNVD-2017-28238、CNVD-2017-28274）。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-2017-28240
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28247
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28250

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28284

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28285

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28283

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28238

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28274

### 3、Oracle 产品安全漏洞

Oracle PeopleSoft Products 是美国甲骨文公司的一套企业人力资本管理解决方案。Java SE 是用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序，Java SE Embedded 是一款针对嵌入式系统开发功能的应用程序的 Java 平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未授权读取、更新、插入或删除数据，影响数据的保密性、可用性和完整性。

CNVD 收录的相关漏洞包括：Oracle Java SE 和 Java SE Embedded 存在未明漏洞（CNVD-2017-28398、CNVD-2017-28399、CNVD-2017-28400、CNVD-2017-28402、CNVD-2017-28403）、Oracle PeopleSoft Enterprise PRTL Interaction Hub 未授权操作漏洞（CNVD-2017-28221、CNVD-2017-28370、CNVD-2017-28378）。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-2017-28398

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28399

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28400

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28402

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28403

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28221

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28370

http://www.cnvd.org.cn/flaw/show/CNVD-2017-28378

### 4、Adobe 产品安全漏洞

Adobe Experience Manager 是美国 Adobe 公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。Adobe Reader 是 PDF 文档阅读软件。Acrobat 是 PDF 文档编辑软件。Adobe Flash Player 是一款跨平台、基于浏览器的多媒体播放器产品。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制、执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 安全绕过漏洞（CNVD-2017-28430）、Adobe Acrobat/Reader 内存破坏漏洞（CNVD-2017-28443）、Adobe Acrobat/Reader 远程代码执行漏洞（CNVD-2017-28431、CNVD-2017-28433、CNVD-2017-28434、CNVD-2017-28435）、Adobe Experience Manager 任意代码执行漏洞、Adobe Flash Playe

r 类型混淆远程执行代码漏洞。除“Adobe Acrobat/Reader 安全绕过漏洞（CNVD-2017-28430）、Adobe Acrobat/Reader 内存破坏漏洞（CNVD-2017-28443）”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-2017-28430
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28443
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28431
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28433
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28434
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28435
http://www.cnvd.org.cn/flaw/show/CNVD-2017-28750
http://www.cnvd.org.cn/flaw/show/CNVD-2017-27994

### 5、finecms SQL 注入漏洞（CNVD-2017-28415）

FineCMS 是一款基于 PHP+MySql+CI 框架开发的建站系统。本周，FineCMS 被披露存在 SQL 注入漏洞，远程攻击者可利用漏洞操作网站数据库。目前，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-2017-28415

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-2017-27984 | WordPress Loginizer SQL 注入漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://sv.wordpress.org/plugins/loginizer/#developers |
| CNVD-2017-27999 | Apache Xerces-C++拒绝服务漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://bugzilla.redhat.com/show_bug.cgi?id=787103 |
| CNVD-2017-28225 | rest-client 会话固定漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://bugzilla.redhat.com/show_bug.cgi?id=1205291 |
| CNVD-2017-28257 | Adiscon rsyslog zmq3 输入和输出模块字符串漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/rsyslog/rsyslog/pull/1565 |
| CNVD-2017-28409 | HashiCorp Vagrant VMware Fusion 插件任意代码执行漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： |

| | | | |
|---|---|---|---|
| | | | https://www.vagrantup.com/ |
| CNVD-2017-28619 | Xen 内存破坏漏洞（CNVD-2017-28619） | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://xenbits.xen.org/xsa/advisory-229.html |
| CNVD-2017-28621 | Xen map_grant_ref 权限提升漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://xenbits.xen.org/xsa/advisory-227.html |
| CNVD-2017-28744 | ONOS 跨站脚本漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://gerrit.onosproject.org/#/c/14031/ |
| CNVD-2017-28785 | Haxx curl/libcURL 堆缓冲区溢出漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://curl.haxx.se/docs/adv_20170809B.html |
| CNVD-2017-28792 | Apple iOS 缓冲区溢出漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：http://seclists.org/fulldisclosure/2017/Jul/34 |

表 4 部分重要高危漏洞列表

小结：本周，Microsoft 被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码。此外，Tcpdump、Oracle、Adobe 多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制、执行任意代码或发起拒绝服务攻击等。另外，FineCMS 被披露存在 SQL 注入漏洞，远程攻击者可利用漏洞操作网站数据库。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. Discuz! 任意文件删除漏洞

Crossday Discuz! Board（简称 Discuz!）是北京康盛新创科技有限责任公司推出的一套通用的开源的社区论坛软件系统。采用 PHP 和 MySQL 构建的性能优异、功能全面的社区论坛平台。利用特殊构造的请求触发可参与文件删除操作，导致了任意文件删除漏洞的发生。

参考链接：http://www.freebuf.com/vuls/149762.html

### 2. 主板厂商利用英特尔 UEFI BIOS 固件漏洞留后门

Cylance 的安全研究员 Alex Matrosov 发现了一些主板厂商利用英特尔的 UEFI BIOS 固件几个漏洞留后门。这些漏洞允许攻击者绕过 BIOS 固件保护，例如 Intel Boot

Guard 和 Intel BIOS Guard，以禁用和更改 UEFI BIOS 固件，例如放置 rootkit。

参考链接：https://95cnsec.com/motherboards-bios-flaws.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