

信息安全漏洞周报

2016 年 12 月 19 日-2016 年 12 月 25 日

2016 年第 52 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 360 个，其中高危漏洞 137 个、中危漏洞 196 个、低危漏洞 27 个。漏洞平均分为 6.03。本周收录的漏洞中，涉及 0day 漏洞 67 个（占 19%）。其中互联网上出现“Samsung KNOX 堆栈缓冲区溢出漏洞、Roundcube 远程代码执行漏洞（CNVD-2016-12559）”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 575 个，与上周（734 个）环比下降 22%。

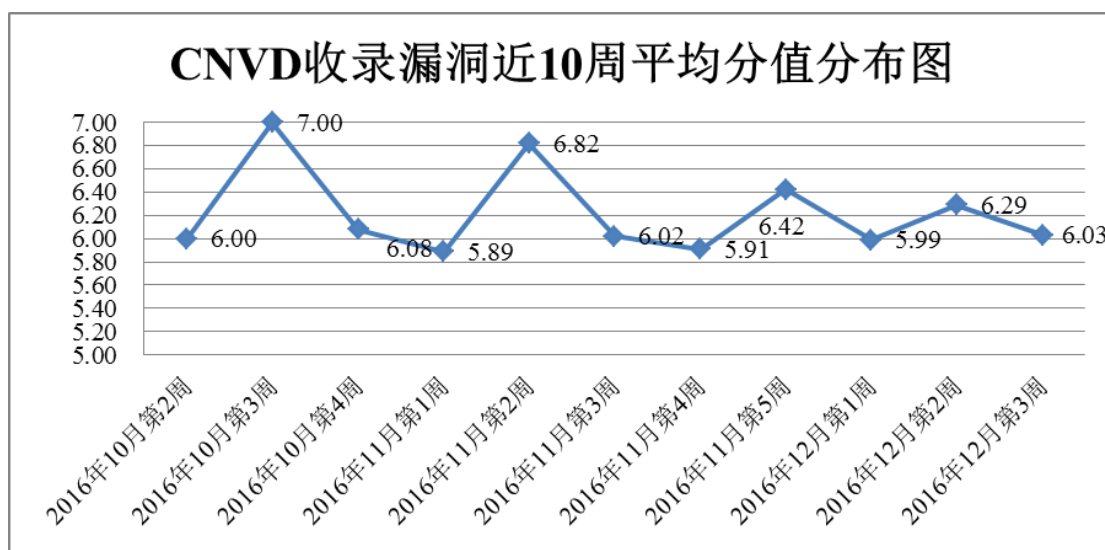


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 11 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 360 漏洞。报送情况如表 1 所示。其中，安天实验室、天融信、华为技术有限公司、恒安嘉新等单位报送数量较多。360 网神、漏洞盒子、南京铨迅信息技术股份有限公司、西

安四叶草信息技术有限公司、广西鑫瀚科技有限公司、福建六壬网安股份有限公司、清远职业技术学院、广州圣辉信息技术有限公司及其他个人白帽子向 CNVD 提交了 575 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	509	509
安天实验室	210	0
天融信	202	0
华为技术有限公司	101	0
恒安嘉新	86	4
H3C	62	0
杭州安恒信息技术有 限公司	58	0
蓝盾信息安全技术股 份有限公司	52	0
绿盟科技	45	0
北京数字观星科技有 限公司	5	0
南京铨迅信息技术股 份有限公司	4	4
漏洞盒子	20	20
西安四叶草信息技 术有限公司	10	10
广西鑫瀚科技有限公 司	5	5
福建六壬网安股份有 限公司	3	3
清远职业技术学院	3	3
广州圣辉信息技 术有限公司	2	2
国家互联网应急中心	1	1
CNCERT 新疆分中心	6	6
CNCERT 海南分中心	3	3

CNCERT 广东分中心	2	2
CNCERT 江西分中心	2	2
CNCERT 安徽分中心	1	1
个人	110	110
报送总计	1387	575
录入总计	360（去重）	575

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 360 个漏洞。其中应用程序漏洞 203 个，操作系统漏洞 66 个，web 应用漏洞 56 个，网络设备漏洞 20 个，安全产品漏洞 14 个，数据库漏洞 1 条。

漏洞影响对象类型	漏洞数量
应用程序漏洞	203
操作系统漏洞	66
web 应用漏洞	56
网络设备漏洞	20
安全产品漏洞	14
数据库漏洞	1

表 2 漏洞按影响类型统计表

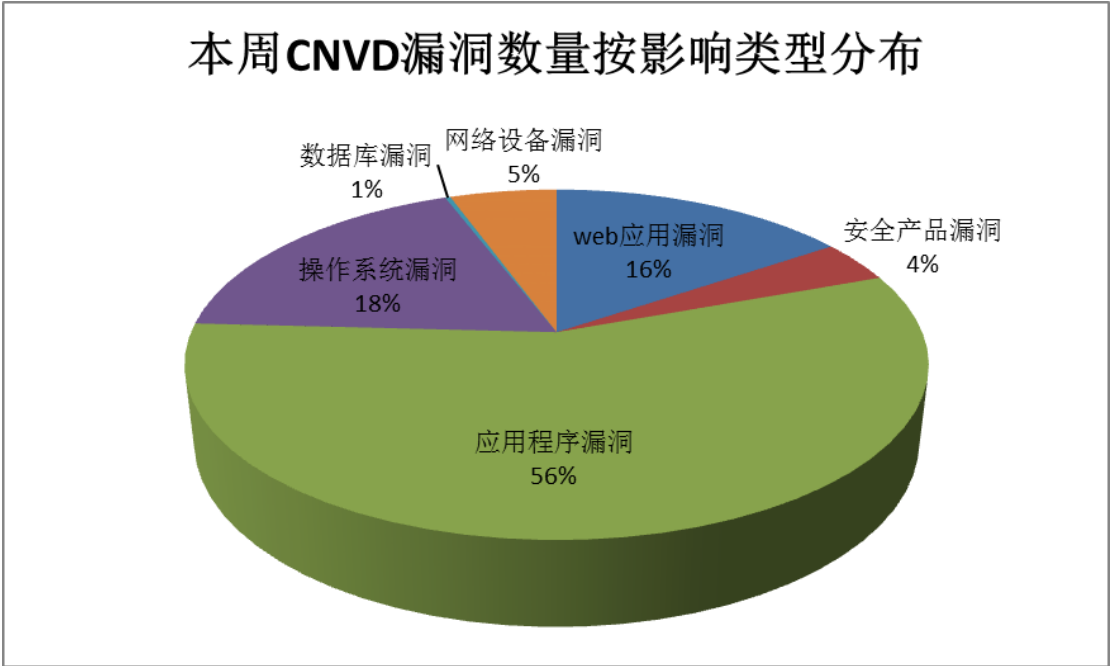


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、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	Apple	82	23%
2	Cisco	20	6%
3	NVIDIA	16	4%
4	Mozilla	14	4%
5	QEMU	11	3%
6	IBM	10	3%
7	McAfee	10	3%
8	Cybozu	8	2%
9	phpMyAdmin	8	2%
10	其他	175	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 10 个电信行业漏洞，65 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，“多款 Delta Electronics 产品堆缓冲区溢出漏洞、多款 Delta Electronics 产品任意文件访问漏洞、Apple iOS APPLE-SA-2016-12-12-1 存在多个漏洞（CNVD-2016-12705、CNVD-2016-12706、CNVD-2016-12707、CNVD-2016-12708、CNVD-2016-12709、CNVD-2016-12710、CNVD-2016-12711、CNVD-2016-12712）”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/>

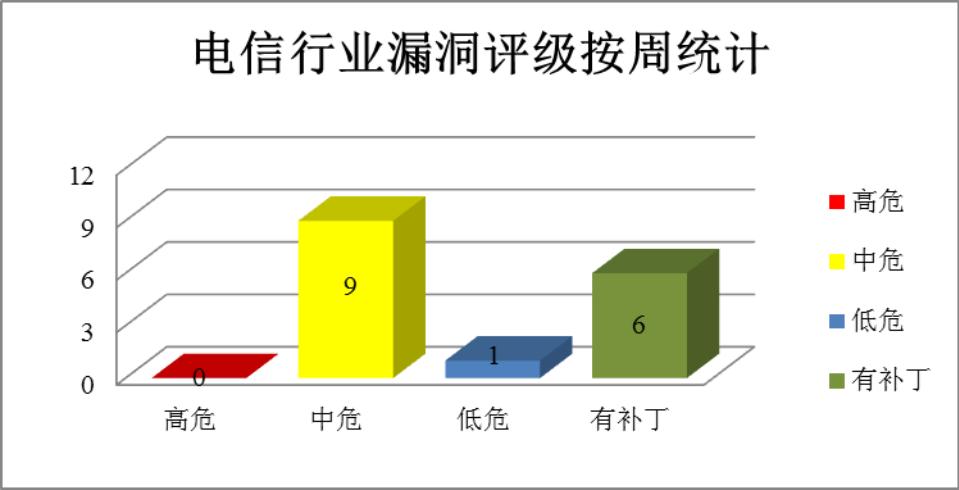


图 3 电信行业漏洞统计

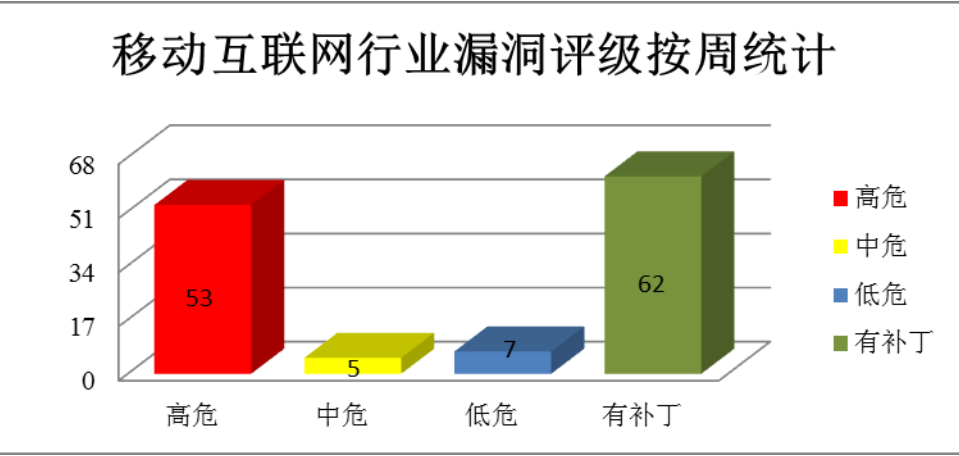


图 4 移动互联网行业漏洞统计

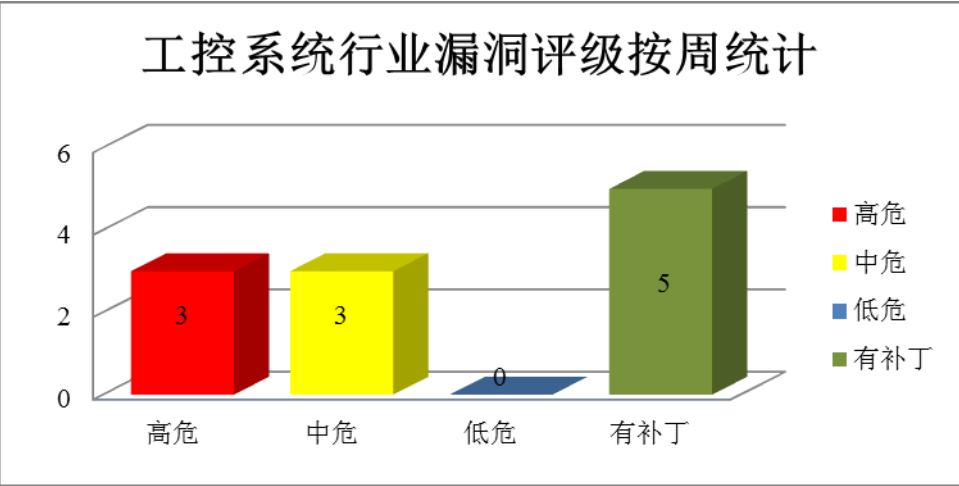


图 5 工控系统行业漏洞统计

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、OpenSSH 产品安全漏洞

OpenSSH (OpenBSD Secure Shell) 是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。本周, 该产品被披露存在多个漏洞, 攻击者可利用漏洞执行任意代码、提升权限、泄露敏感信息或绕过安全限制等。

CNVD 收录的相关漏洞包括: OpenSSH 安全绕过漏洞、OpenSSH 本地信息泄露漏洞、OpenSSH 特权提升漏洞、OpenSSH 远程代码执行漏洞。其中, “OpenSSH 特权提升漏洞”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-2016-12684>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12686>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12687>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12688>

2、Apple 产品安全漏洞

Apple Safari、iCloud for Windows、iTunes、iOS 和 tvOS 都是美国苹果 (Apple) 公司的产品。Apple Safari 是一款 Web 浏览器, 是 Mac OS X 和 iOS 操作系统附带的默认浏览器; iTunes 是一套媒体播放器应用程序。WebKit 是 KDE 社区开发的一套开源 Web 浏览器引擎。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代码。

CNVD 收录的相关漏洞包括: 多款 Apple 产品 WebKit 组件内存破坏漏洞 (CNVD-2016-12781、CNVD-2016-12782、CNVD-2016-12783、CNVD-2016-12784、CNVD-2016-12785、CNVD-2016-12786、CNVD-2016-12787、CNVD-2016-12788) 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-2016-12781>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12782>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12783>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12784>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12785>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12786>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12787>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12788>

3、Cisco 产品安全漏洞

Cisco ASR 5000 Series Software 是美国思科 (Cisco) 公司的 5000 系列无线控制器产品。Cisco Email Security Appliance 是一款思科电子邮件安全设备。FireAMP Connector Endpoint Software 是一款安全产品。Cisco Firepower 是高级防火墙系列产品。Cisco Identity Services Engine 是一种转换生成的技术。Cisco Prime Collaboration Assuran

ce 是一款视频和语音服务解决方案。Cisco Unified Communications Manager 是一款统一通信系统中的呼叫处理组件。本周，上述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或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco ASR 5000 Series 拒绝服务漏洞（CNVD-2016-12775）、Cisco Email Security Appliance 安全绕过漏洞（CNVD-2016-12543）、Cisco FireAMP Connector Endpoint Software 本地拒绝服务漏洞、Cisco FirePOWER Malware 安全绕过漏洞、Cisco Firepower Management Center 信息泄露漏洞（CNVD-2016-12547）、Cisco Identity Services Engine 跨站脚本漏洞（CNVD-2016-12550）、Cisco Prime Collaboration Assurance 跨站脚本漏洞（CNVD-2016-12549）、Cisco Unified Communications Manager 跨站脚本漏洞等。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-2016-12775>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12543>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12583>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12545>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12547>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12550>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12549>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12769>

4、Mozilla 产品安全漏洞

Mozilla Firefox 和 Firefox ESR 都是美国 Mozilla 基金会开发的浏览器产品。Firefox 是一款开源 Web 浏览器；Firefox ESR 是 Firefox 的一个延长支持版本。本周，上述产品被披露存在多个漏洞，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：Mozilla Firefox SkiaGL 缓冲区溢出漏洞、Mozilla Firefox WebVR 内存错误引用漏洞、Mozilla Firefox 存在未明漏洞（CNVD-2016-12657）、Mozilla Firefox 内存破坏漏洞（CNVD-2016-12691、CNVD-2016-12697）、Mozilla Firefox 任意代码执行漏洞（CNVD-2016-12690、CNVD-2016-12693、CNVD-2016-12699）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-2016-12654>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12655>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12657>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12691>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12697>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12690>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12693>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12699>

5、Microsoft Remote Desktop Client for Mac 远程代码执行漏洞

Microsoft Remote Desktop 是微软官方推出的连接 Windows 远程桌面的移动端客户端。本周，Microsoft 被披露存在远程代码执行漏洞。攻击者利用漏洞可在受影响的进程中执行任意代码。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-2016-12567>

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-2016-12577	Drupal JavaScript Callback Handler 存在未明安全绕过漏洞	高	用户可联系供应商获得补丁信息： https://www.drupal.org/node/2833790
CNVD-2016-12614	WordPress 插件 Google Analytics Counter Tracker PHP 对象注入漏洞	高	用户可联系供应商获得补丁信息： https://wordpress.org/plugins/analytics-counter/
CNVD-2016-12617	Joomla extension DT Register SQL 注入漏洞	高	用户可联系供应商获得补丁信息： https://extensions.joomla.org/extension/dt-register
CNVD-2016-12629	McAfee VirusScan Enterprise 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.kb.cert.org/vuls/id/245327
CNVD-2016-12627	McAfee VirusScan Enterprise 安全绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.kb.cert.org/vuls/id/245327
CNVD-2016-12626	McAfee VirusScan Enterprise 安全绕过漏洞（CNVD-2016-12626）	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.kb.cert.org/vuls/id/245327
CNVD-2016-12625	McAfee VirusScan Enterprise CRLF 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.kb.cert.org/vuls/id/245327
CNVD-2016-12624	McAfee VirusScan Enterprise SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.kb.cert.org/vuls/id/245327

CNVD-2016-12889	FlightGear 任意文件覆盖漏洞	高	用户可联系供应商获得补丁信息： http://www.flightgear.org/about/
CNVD-2016-12894	Red Hat Rosteasy 远程代码执行漏洞	高	用户可联系供应商获得补丁信息： https://www.redhat.com/en

表 4 部分重要高危漏洞列表

小结：本周，OpenSSH 被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权限、泄露敏感信息或绕过安全限制等。此外，Apple、Cisco、Mozilla 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码、绕过安全限制或发起拒绝服务攻击等。另外，Microsoft 被披露存在远程代码执行漏洞。攻击者利用漏洞可在受影响的进程中执行任意代码。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. 流行开源电子邮件程序 Roundcube v1.2.2 命令执行漏洞分析

Roundcube 是一款被广泛使用的开源的电子邮件程序，在全球范围内有很多组织和公司都在使用。在过去的 1 年里，仅 SourceForge 上的镜像文件被下载次数就超过 26 万，这还仅仅是实际使用群体中的一小部分。在服务器上成功安装 Roundcube 之后，它会提供给用户一个 web 接口，通过验证的用户就可以通过 Web 浏览器收发电子邮件。在 Roundcube1.2.2 或者更早的版本里，用户的输入未经过滤就被传到了 PHP 内建函数 mail() 的第五个参数，攻击者可以利用此选项在网站根目录下创建一个恶意 PHP 文件，以下代码可触发漏洞。由于使用默认安装方式的 Roundcube 都受影响，所以我们强烈建议使用 Roundcube 的管理员尽快更新到 1.2.3 版本。

参考链接：<http://www.freebuf.com/vuls/122658.html>

2. 一个和任天堂游戏机有关的 0-day 漏洞

上个月 Chris Evans 陆续针对 Linux 系统中的 GStreamer 框架进行了安全分析，发现了针对 Linux 桌面系统的 0-day 漏洞。最近，Evans 公开了稳定版的漏洞 exploit，可利用特制音频文件的隐蔽下载（drive-by download）实现 Linux 系统入侵。目前，该漏洞可能还将对其它 Linux 发行版本造成影响。执行攻击的特制音频文件包含恶意代码，可以针对用户实现隐蔽（drive-by download）下载，一旦成功加载之后，攻击者可以通过其执行一系列与当前系统用户权限相当的操作。通过该攻击，可以窃取所有用户数据信息，包括照片、视频、文档和浏览器 cookie 等。

参考链接：<http://www.freebuf.com/news/123521.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