

信息安全漏洞周报

2016 年 10 月 31 日-2016 年 11 月 06 日

2016 年第 45 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 239 个，其中高危漏洞 69 个、中危漏洞 153 个、低危漏洞 17 个。漏洞平均分为 5.89。本周收录的漏洞中，涉及 0day 漏洞 41 个（占 17%）。其中互联网上出现“CherryTree 内存破坏漏洞、Wordpress Userpro 插件文件上传漏洞”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 1000 个，与上周（786 个）环比增长 27%。

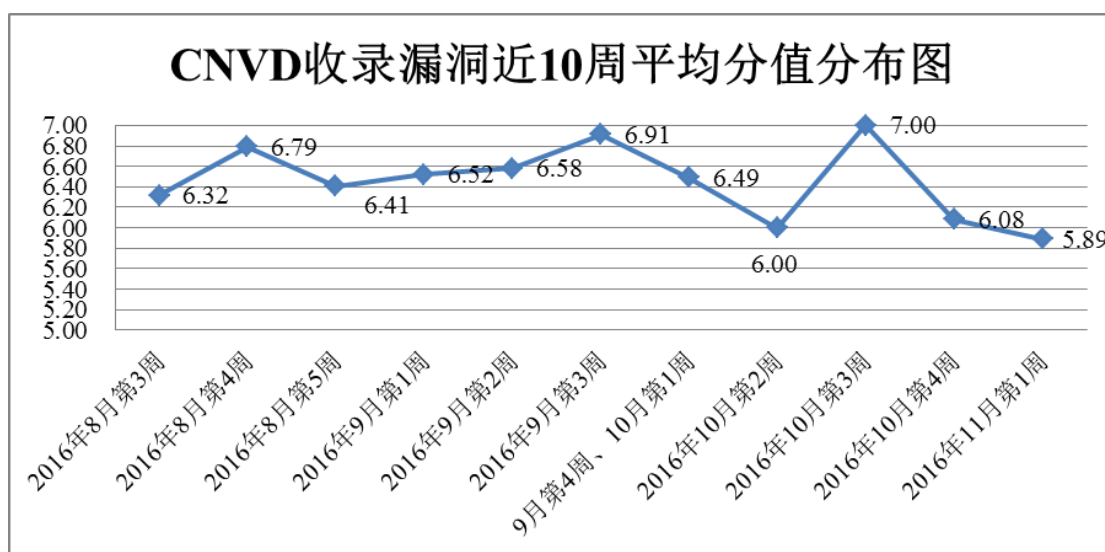


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 12 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 239 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、绿盟科技、蓝盾信息安全技术有限公司、恒安嘉新等单位报送数量较多。奇虎（补天平台）、漏洞盒子、广

西鑫瀚科技有限公司、西安四叶草信息技术有限公司、上海零盾网络科技有限公司、上海云盾信息技术有限公司、广州圣辉信息技术有限公司、南京铭迅信息技术有限公司、新疆天山智汇信息科技有限公司、广东电网有限责任公司电力科学研究院、北京禹宏信安科技有限公司、西安瑞天信息安全技术有限公司及其他个人白帽子向 CNVD 提交了 1000 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
奇虎（补天平台）	753	753
启明星辰	133	23
安天实验室	119	0
绿盟科技	103	0
蓝盾信息安全技术有限公司	104	0
恒安嘉新	64	3
华为技术有限公司	50	0
杭州安恒信息技术有限公司	40	0
H3C	34	2
中国电信集团系统集成有限责任公司	27	0
卫士通信息产业股份有限公司	8	0
知道创宇	1	0
漏洞盒子	132	132
广西鑫瀚科技有限公司	29	29
西安四叶草信息技术有限公司	10	10
上海零盾网络科技有限公司	6	6
上海云盾信息技术有限公司	5	5
广州圣辉信息技术有限公司	4	4

南京铨迅信息技术股份有限公司	3	3
新疆天山智汇信息科技有限公司	2	2
广东电网有限责任公司电力科学研究院	1	1
北京禹宏信安科技有限公司	1	1
西安瑞天信息安全技术有限公司	1	1
CNCERT 宁夏分中心	2	2
CNCERT 上海分中心	1	1
CNCERT 天津分中心	1	1
个人	21	21
报送总计	1655	1000
录入总计	239（去重）	1000

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 239 个漏洞。其中应用程序漏洞 163 个，web 应用漏洞 24 个，网络设备漏洞 24 个，操作系统漏洞 22 个，安全产品漏洞 5 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	163
web 应用漏洞	24
网络设备漏洞	24
操作系统漏洞	22
安全产品漏洞	5
数据库漏洞	1

表 2 漏洞按影响类型统计表

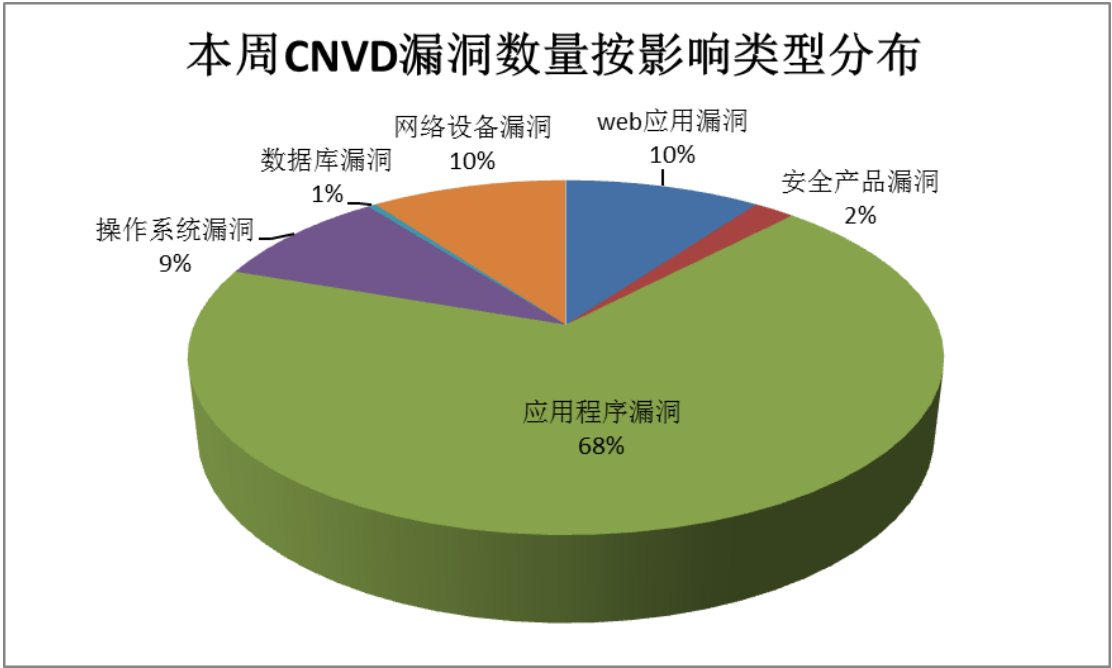


图 2 本周漏洞按影响类型分布

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	22	9%
2	Cisco	20	8%
3	NVIDIA	16	7%
4	OpenJPEG	7	3%
5	Foxit	7	3%
6	Apache	6	3%
7	iTrack	5	2%
8	IBM	4	2%
9	QEMU	4	2%
10	其他	149	61%

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 15 个电信行业漏洞，20 个移动互联网行业漏洞，9 个工控系统行业漏洞（如下图所示）。其中，“Samsung Galaxy S4 至 S7 设备未授权修改漏洞、多款 Apple 产品 CoreGraphics 内存破坏漏洞、多款 Apple 产品 WebKit 内存破坏漏洞、

多款 Apple 产品 libxpc 任意代码执行漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2016-10367）、musl libc 'tre_tnfa_run_parallel()'函数整数溢出漏洞、IBHsoftec S7-SoftPLC CPX43 堆缓冲区溢出漏洞、ABB RobotWare 身份验证漏洞、ABB RobotWare 远程代码执行漏洞、Schneider Electric Unity PRO 远程代码执行漏洞”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/>

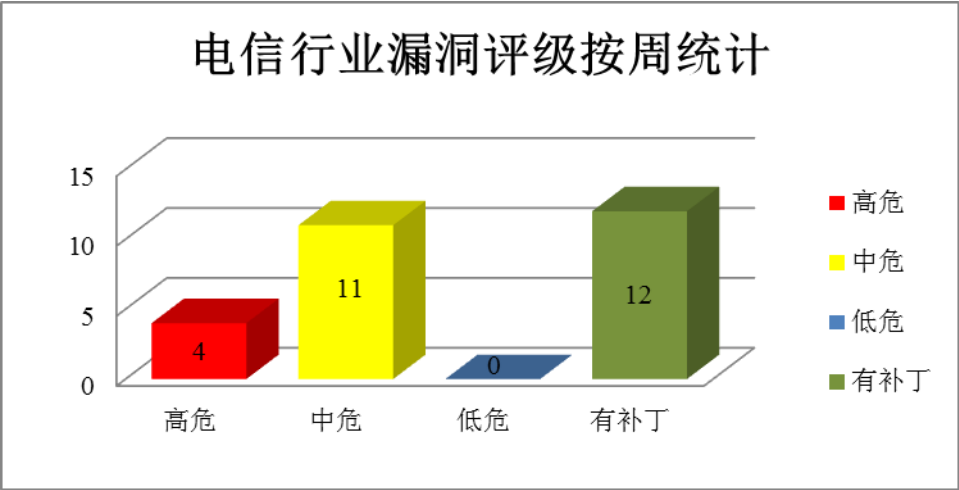


图 3 电信行业漏洞统计

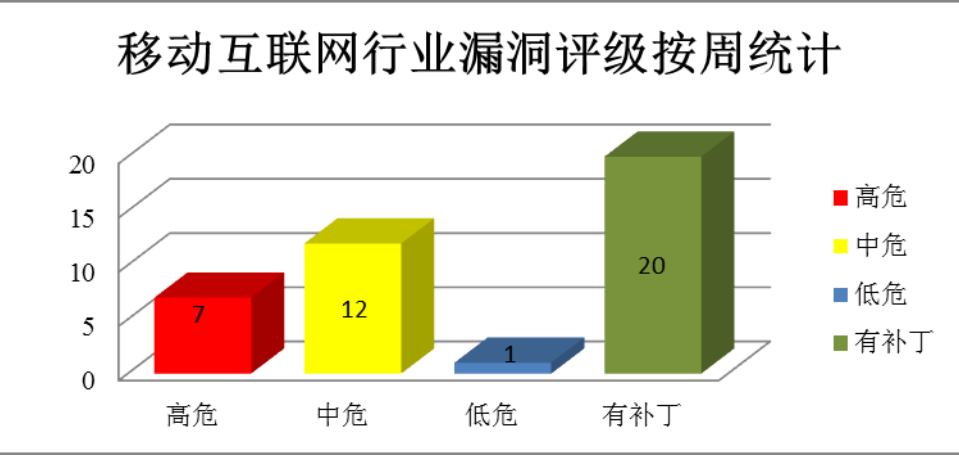


图 4 移动互联网行业漏洞统计

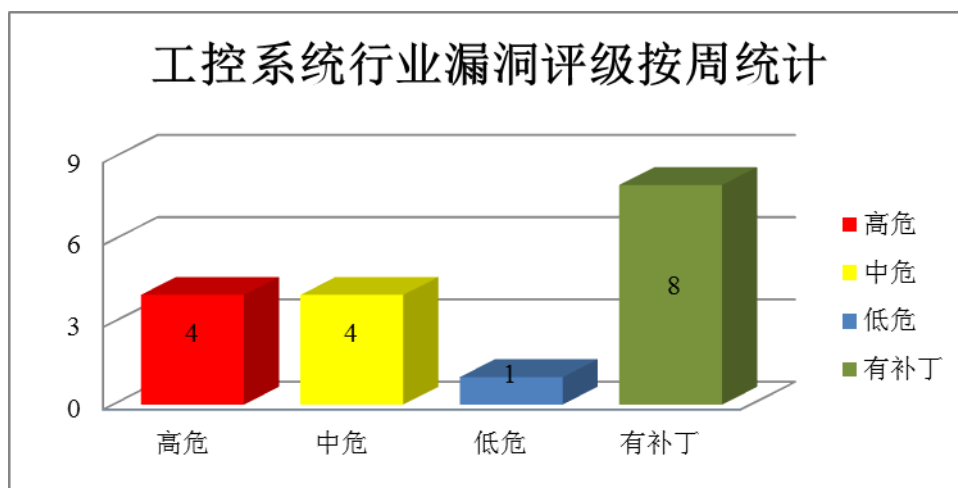


图 5 工控系统行业漏洞统计

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、Apple 产品安全漏洞

Apple macOS Sierra 是为 Mac 计算机所开发的一套专用操作系统。CoreGraphics 是一个 iOS 内置的绘图框架组件。Apple iOS、Safari 和 tvOS 都是美国苹果（Apple）公司的产品。WebKit 是 KDE 社区开发的一套开源 Web 浏览器引擎。watchOS 是一套智能手表操作系统。libxpc 是其中的一个 Apple XPC 库的开源实现。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或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Apple macOS Sierra ATS 内存破坏漏洞、Apple macOS Sierra NVIDIA Graphics Drivers 内存破坏漏洞、Apple macOS Sierra AppleGraphicsControl 内存破坏漏洞、多款 Apple 产品 CoreGraphics 内存破坏漏洞、Apple macOS Sierra ImageIO 越边界写入漏洞、多款 Apple 产品 WebKit 内存破坏漏洞、多款 Apple 产品 libxpc 任意代码执行漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2016-10367）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-2016-10372>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10355>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10371>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10408>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10373>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10412>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10409>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10367>

2、Cisco 产品安全漏洞

Cisco Meeting Server 是美国思科（Cisco）公司的一套包含音频、视频的会议服务器软件。Cisco AsyncOS 操作系统是可以提升思科电子邮件安全设备的安全性和性能。Cisco ASR 5000 系列是一个运营商级平台。Cisco Application Policy Infrastructure Controller 是一款自动化管理以应用为中心的基础设施（ACI）的控制器。Cisco ASR 900 系列是模块化聚合服务路由器。本周，该产品被披露存在缓冲区溢出和拒绝服务漏洞，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：Cisco Application Policy Infrastructure Controller 拒绝服务漏洞、Cisco ASR 900 Series Aggregation Services Routers 缓冲区溢出漏洞、Cisco Meeting Server 和 Meeting App 缓冲区溢出漏洞、Cisco AsyncOS 拒绝服务漏洞（CNVD-2016-10393、CNVD-2016-10394、CNVD-2016-10395）、Cisco ASR 5500 Series Routers 拒绝服务漏洞、Cisco Meeting Server SDP 解析器缓冲区溢出漏洞等。除“Cisco ASR 5500 Series Routers 拒绝服务漏洞、Cisco Meeting Server SDP 解析器缓冲区溢出漏洞”外漏洞的综合评级为“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-2016-10622>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10615>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10610>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10393>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10394>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10395>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10623>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10614>

3、Foxit 产品安全漏洞

Foxit Reader 是中国福昕（Foxit）软件公司的一款 PDF 文档阅读器。Foxit PhantomPDF 是一个商业版。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、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：Foxit Reader 任意代码执行漏洞（CNVD-2016-10596）、Foxit Reader 和 PhantomPDF 拒绝服务漏洞（CNVD-2016-10514、CNVD-2016-10510）、Foxit Reader 和 PhantomPDF 越边界读取漏洞（CNVD-2016-10513、CNVD-2016-10512）、Foxit Reader 和 PhantomPDF 缓冲区溢出漏洞（CNVD-2016-10511）、Foxit Reader 边界读取本地信息泄露漏洞等。其中，“Foxit Reader 任意代码执行漏洞（CNVD-2016-10596）”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-2016-10596>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10514>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10513>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10512>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10511>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10510>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10360>

4、Apache 产品安全漏洞

Apache CloudStack 是部署和管理大型虚拟机网络的开源软件。Apache Tomcat 是一个流行的开源 JSP 应用服务器程序。本周，上述产品被披露存在安全限制绕过和信息泄露漏洞，攻击者可利用漏洞泄露敏感信息或绕过安全限制。

CNVD 收录的相关漏洞包括：Apache CloudStack 授权绕过漏洞、Apache Tomcat 安全限制绕过漏洞（CNVD-2016-10419）、Apache Tomcat 信息泄露漏洞（CNVD-2016-10420）、Apache Tomcat Security Manager 安全限制绕过漏洞（CNVD-2016-10421、CNVD-2016-10423）、Apache Tomcat 安全限制绕过漏洞。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-2016-10519>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10419>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10420>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10421>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10422>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-10423>

5、多款 Schneider Electric 产品拒绝服务漏洞

Schneider Electric Magelis HMI Magelis GTO Advanced Optimum panels 等都是法国施耐德电气（Schneider Electric）公司的 HMI 人机面板系列产品。本周，Schneider Electric 被披露存在拒绝服务漏洞。攻击者利用漏洞可破坏目标 web 服务器，导致服务器拒绝服务，设备重启。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-2016-10624>

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-2016-10448	Nginx 远程权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://nginx.org/
CNVD-2016-10455	Firejail 远程权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：

			https://firejail.wordpress.com/
CNVD-2016-10450	Network Scanner 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://www.mitec.cz/
CNVD-2016-10468	Memcached Append/Prepend 存在远程代码执行漏洞	高	厂商已发布新版本修复该漏洞，请升级至官方最新版本： http://www.memcached.org/files/memcached-1.4.33.tar.gz
CNVD-2016-10467	Memcached Update 存在远程代码执行漏洞	高	厂商已发布新版本修复该漏洞，请升级至官方最新版本： http://www.memcached.org/files/memcached-1.4.33.tar.gz
CNVD-2016-10466	Memcached SASL 存在身份验证远程代码执行漏洞	高	厂商已发布新版本修复该漏洞，请升级至官方最新版本： http://www.memcached.org/files/memcached-1.4.33.tar.gz
CNVD-2016-10474	多个 Synology DiskStation 产品不安全默认密码漏洞	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.synology.com/
CNVD-2016-10523	NVIDIA Driver 缺少边界检查漏洞	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://nvidia.custhelp.com/app/answers/detail/a_id/4247
CNVD-2016-10521	Linux Kernel Vfiio Driver 整数溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://patchwork.kernel.org/patch/9373631/
CNVD-2016-10533	NVIDIA GeForce Experience 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.nvidia.com/object/product-security.html

表 4 部分重要高危漏洞列表

小结：本周，Apple 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等。此外，Cisco、Foxit、Apache 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、绕过安全限制、执行任意代码和发起拒绝服务攻击等。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. MySQL 现高危漏洞，可致服务器 root 权限被窃取

上周，一位名叫 Dawid Golunski 的波兰黑客发现了存在于 MySQL 中的漏洞：一个远程 root 代码执行漏洞和一个权限提升漏洞。它能够让一个低权限账号（拥有 CREAT

E/INSERT/SELECT 权限)提升权限并且以系统用户身份执行任意代码。导致这个问题的原因其实是因为 MySQL 对错误日志以及其他文件的处理不够安全, 这些文件可以被替换成任意的系统文件, 从而被利用来获取 root 权限。所有的这些漏洞都可以在共享环境中使用。在共享环境中, 用户能够访问各自独立的数据库。而通过这些漏洞, 黑客可以获取到所有数据库的权限。

参考链接: <http://www.freebuf.com/news/119022.html>

2. 施耐德工业防火墙被爆严重安全漏洞

根据国外媒体的最新报道, 工业安全公司 CyberX 的安全研究专家在 2016 年工业控制系统 (ICS) 网络安全大会上披露了好几个严重的安全漏洞, 安全研究专家在对施耐德 ConneXium 工业级以太网防火墙进行安全检测时, 在该系列防火墙产品的 Web 管理接口中发现了一个缓冲区溢出漏洞。如果能够成功利用该漏洞的话, 那么攻击者将可以在目标设备中远程执行任意代码。攻击者可以利用这个漏洞来修改目标设备的防火墙规则、窃听网络数据、注入恶意流量。

参考链接: <http://www.freebuf.com/news/118167.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