

信息安全漏洞周报

2017 年 10 月 30 日-2017 年 11 月 05 日

2017 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 455 个，其中高危漏洞 97 个、中危漏洞 316 个、低危漏洞 42 个。漏洞平均分为 5.67。本周收录的漏洞中，涉及 0day 漏洞 105 个（占 23%），其中互联网上出现“3CX Phone System 目录遍历漏洞、Flexense VX Search Enterprise 缓冲区溢出漏洞”零日代码攻击漏洞。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 832 个，与上周（853 个）环比下降 2%。

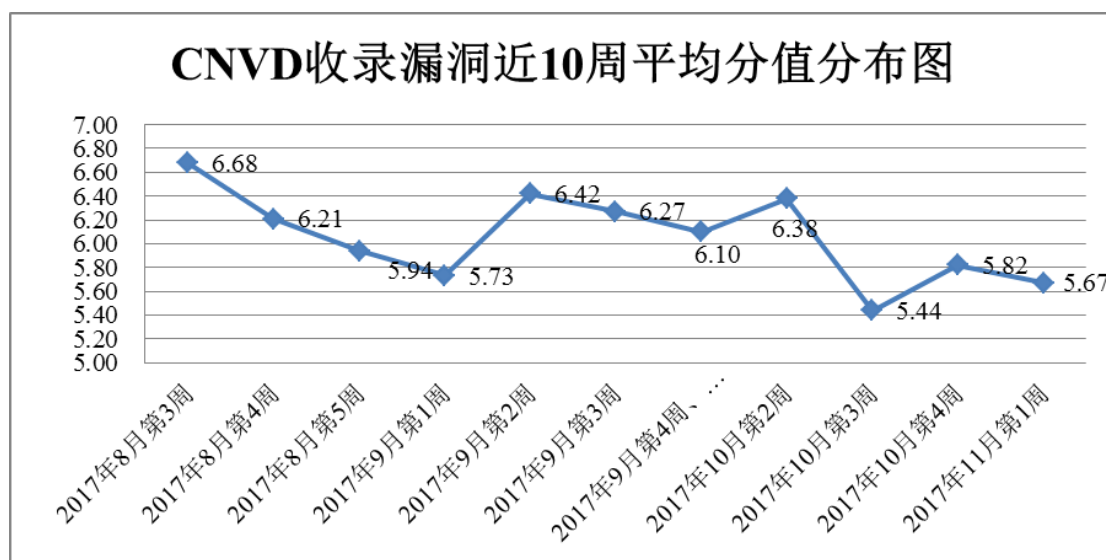


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，华为技术有限公司、H3C、安天实验室、天融信、恒安嘉新等单位报送数量较多。深圳市鼎安天下信息科技有限公司、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、南京联成科技发展股份有

限公司君立华域、福建榕基软件股份有限公司、安元实验室、广州万方计算机科技有限公司、网信智安、福建省海峡信息技术公司及其他个人白帽子向 CNVD 提交了 853 个以事件型漏洞为主的原创漏洞。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
华为技术有限公司	346	0
H3C	324	0
安天实验室	218	0
漏洞盒子	183	183
恒安嘉新	186	0
天融信	181	1
360 网神	145	145
北京数字观星科技有限公司	52	0
杭州安恒信息技术有限公司	50	0
中国电信集团系统集成有限责任公司	38	0
绿盟科技	35	0
启明星辰	15	15
北京无声信息技术有限公司	6	0
厦门服云信息科技有限公司	6	0
东软	1	1
知道创宇	1	0
深圳市鼎安天下信息科技有限公司	25	25
四川虹微技术有限公司 (子午攻防实验室)	13	13
中新网络信息安全股份有限公司	10	10

南京联成科技发展股份有限公司	7	7
君立华域	7	7
福建榕基软件股份有限公司	4	4
安元实验室	3	3
广州万方计算机科技有限公司	2	2
网信智安	1	1
福建省海峡信息技术公司	1	1
CNCERT 山西分中心	18	18
CNCERT 新疆分中心	6	6
CNCERT 吉林分中心	6	6
CNCERT 安徽分中心	3	3
CNCERT 福建分中心	3	3
CNCERT 浙江分中心	2	2
CNCERT 广东分中心	1	1
CNCERT 宁夏分中心	1	1
个人	374	374
报送总计	2274	832

本周漏洞按类型和厂商统计

本周，CNVD 收录了 455 个漏洞。其中应用程序漏洞 294 个，操作系统漏洞 63 个，web 应用漏洞 40 个，网络设备漏洞 29 个，数据库漏洞 24 个，安全产品漏洞 5 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序漏洞	294
操作系统漏洞	63
web 应用漏洞	40
网络设备漏洞	29

数据库漏洞	24
安全产品漏洞	5

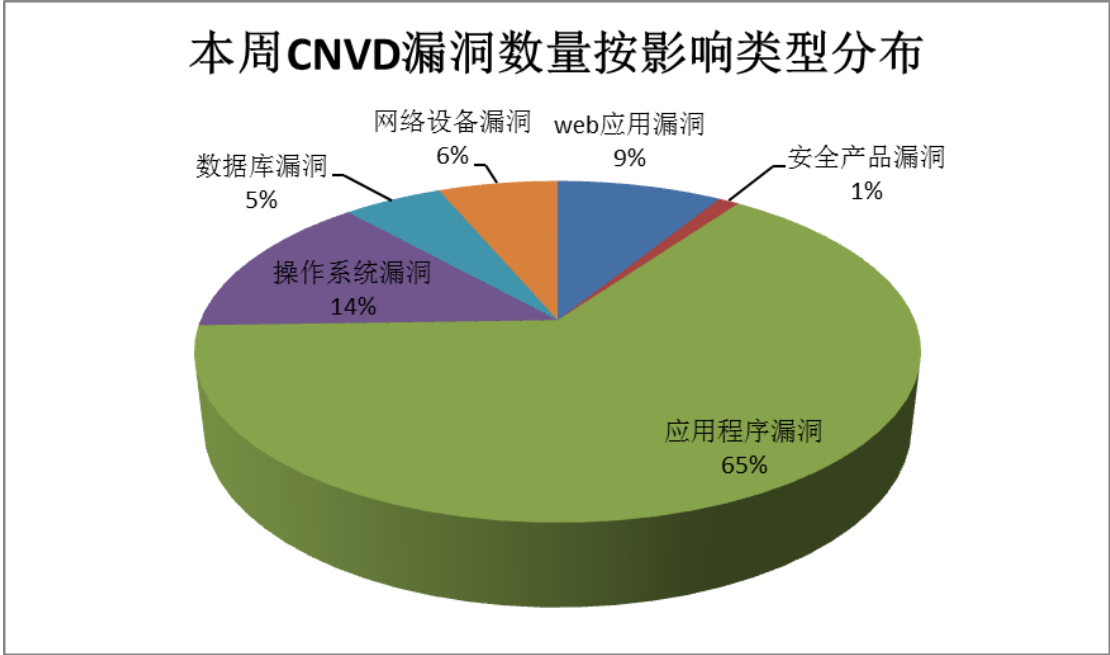


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Cisco、Apple 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	Oracle	58	13%
2	Cisco	40	9%
3	Apple	33	7%
4	XnView	33	7%
5	IrfanView	28	6%
6	Google	17	4%
7	Microsoft	17	4%
8	Mozilla	17	4%
9	Redmine	11	2%
10	其他	201	44%

本周行业漏洞收录情况

本周，CNVD 收录了 30 个电信行业漏洞，57 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，“Advantech WebAccess 指针引用漏洞、Siemens SIMATIC PCS 7 拒绝服务漏洞、Moxa SoftCMS Live Viewer SQL 注入漏洞、D-Link D

IR-600L 会话固定漏洞、Apple iOS Exchange ActiveSync 验证漏洞”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/>

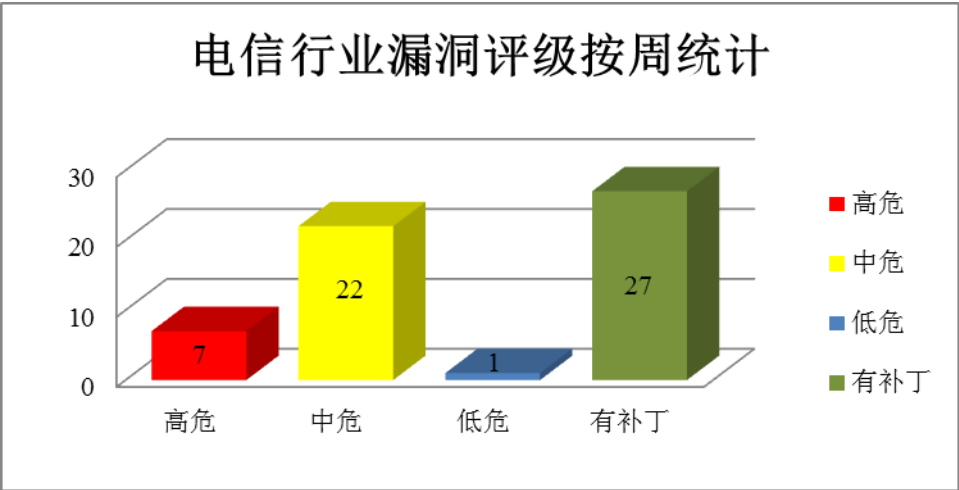


图 3 电信行业漏洞统计

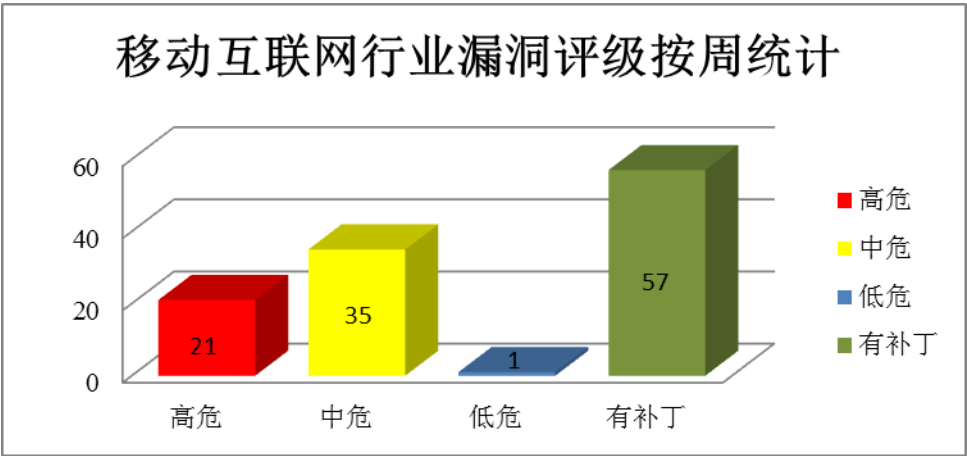


图 4 移动互联网行业漏洞统计

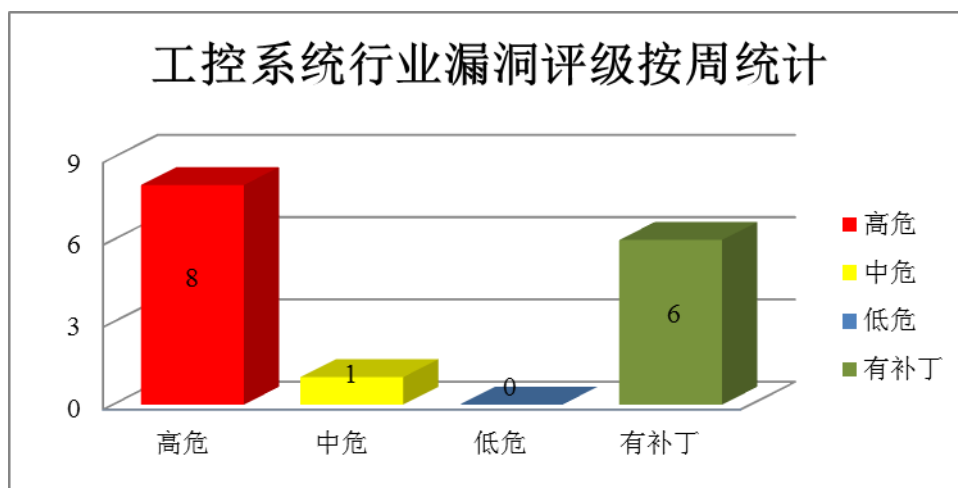


图 5 工控系统行业漏洞统计

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、Apple 产品安全漏洞

Apple iOS 等都是美国苹果公司的产品。Apple iOS 是为移动设备所开发的一套操作系统；tvOS 是一套智能电视操作系统。SQLite 是其中的一套基于 C 语言的开源嵌入式关系数据库管理组件。本周，上述产品被披露存在远程代码执行和缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Apple iOS Wi-Fi 组件任意代码执行漏洞、Apple iOS Wi-Fi 组件任意代码执行漏洞（CNVD-2017-32728、CNVD-2017-32729、CNVD-2017-32730、CNVD-2017-32731、CNVD-2017-32732）、多款 Apple 产品 SQLite 缓冲区溢出漏洞（CNVD-2017-32737、CNVD-2017-32738）。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-2017-32727>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32728>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32729>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32730>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32731>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32732>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32737>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32738>

2、Google 产品安全漏洞

Android 是美国谷歌公司的一套以 Linux 为基础的开源操作系统。MediaTek auxadc

driver 是其中的一个转换器驱动程序。Broadcom Wi-Fi driver 是其中的一个 Wi-Fi 驱动模块。本周，上述产品被披露存在远程代码执行和权限提升漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Broadcom 组件远程代码执行漏洞、Google Android MediaTek lastbus 权限提升漏洞、Google Android MediaTek libmtkomx vdec 权限提升漏洞、Google Android MediaTek teei 权限提升漏洞、Google Android MediaTek 组件权限提升漏洞（CNVD-2017-32470、CNVD-2017-32471、CNVD-2017-32472、CNVD-2017-32473）。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-2017-32557>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31985>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31979>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31978>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32470>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32471>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32472>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32473>

3、Microsoft 产品安全漏洞

Microsoft Windows 7 等都是美国微软公司发布的操作系统。Microsoft Edge 和 Internet Explorer（IE）都是 Windows 系统附带的 Web 浏览器。Microsoft PowerPoint 2007 SP3 是 Office 套件中的一个文档演示工具；SharePoint Server 2013 SP1 是一套企业业务协作平台；Office Web Apps 2010 SP2 是一套基于 Web 的办公软件套件。Microsoft Office 2007 SP3 等是办公软件套件产品。本周，上述产品被披露存在内存破坏、权限提升和远程代码执行漏洞，攻击者可利用漏洞获取权限或执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Office 内存破坏漏洞（CNVD-2017-32622）、Microsoft Windows Edge 和 Internet Explorer JavaScript 引擎远程代码执行漏洞、Microsoft Windows Edge 和 Internet Explorer 远程内存破坏漏洞、Microsoft Windows Internet Explorer 和 Edge JavaScript 引擎远程代码执行漏洞、Microsoft Windows Internet Explorer 内存破坏漏洞、Microsoft Windows Internet Explorer 远程代码执行漏洞、Microsoft Windows Kernel 'Win32k.sys'本地权限提升漏洞（CNVD-2017-32663）、多款 Microsoft 产品远程代码执行漏洞。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-2017-32622>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32618>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32664>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32625>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32619>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32617>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32663>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32624>

4、Oracle 产品安全漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。MySQL Server 是其中的服务器组件。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：Oracle MySQL Server 拒绝服务漏洞（CNVD-2017-32200、CNVD-2017-32201、CNVD-2017-32203、CNVD-2017-32204、CNVD-2017-32205、CNVD-2017-32206、CNVD-2017-32207、CNVD-2017-32208）。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-2017-32200>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32201>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32203>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32204>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32205>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32206>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32207>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32208>

5、JanTek JTC-200 跨站请求伪造漏洞

JanTek JTC-200 是台信（JanTek）科技公司的一款 TCP/IP 转换器（串口服务器）。本周，JanTek 被披露存在跨站请求伪造漏洞，远程攻击者可利用该漏洞以用户的身份执行未授权的操作。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-2017-32099>

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-2017-32102	GSI WinPAT Portal SQL 注入漏洞	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.gsi-office.de
CNVD-2017-32224	EMC NetWorker 缓冲区溢出漏洞 (CNVD-2017-32224)	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.emc.com
CNVD-2017-32244	SDL_image 缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息： https://www.libsdl.org/
CNVD-2017-32267	Simple DirectMedia Layer 数字错误漏洞	高	用户可联系供应商获得补丁信息： https://www.libsdl.org/
CNVD-2017-32425	KNX ETSMessages monitor (Falcon) 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： https://www.knx.org
CNVD-2017-32426	Aerohive Networks HiveManager Classic 路径名验证漏洞	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.aerohive.com/
CNVD-2017-32691	ImageMagick PersistPixelCache 函数拒绝服务漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： http://www.imagemagick.org/download/beta/
CNVD-2017-32695	Xen 任意代码执行漏洞 (CNVD-2017-32695)	高	厂商已发布了漏洞修复程序，请及时关注更新： http://xenbits.xen.org/xsa/advisory-231.html
CNVD-2017-32698	Xen 'mm.c'远程权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://xenbits.xen.org/xsa/advisory-234.html
CNVD-2017-32736	多款 Apple 产品 SQLite 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://support.apple.com/en-us/HT208144

表 4 部分重要高危漏洞列表

小结：本周，Apple 被披露存在远程代码执行和缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。此外，Google、Microsoft、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或发起拒绝服务攻击等。另外，JanTek 被披露存在跨站请求伪造漏洞，远程攻击者可利用该漏洞以用户的身份执行未授权的操作。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. WordPress 全版本 WPDB SQL 注入漏洞

WordPress 版本 4.8.2 及之前版本受到该漏洞的影响，\$wpdb->prepare()可以接收和

执行不安全的查询，导致潜在的 SQL 注入（SQLi）。WordPress 核心并不容易直接受到这个漏洞的影响。WordPress 4.8.3 中修复了一个重要的 SQL 注入漏洞，这个漏洞于 2017 年 9 月 20 日通过 hackerone 报给 WordPress 官方。用户可以通过点击后台的仪表盘->更新。

参考链接：<http://m.bobao.360.cn/news/detail/4358.html?from=timeline&isappinstalled=0>

2. 船舶通信平台 AmosConnect 被曝后门和 SQL 注入漏洞

E 安全 10 月 28 日讯 最近，全球船只上安装的卫星通信系统 SATCOM 被曝受到两大高危漏洞影响：具有全系统访问权限的隐藏后门账户；登录表单存在 SQL 注入漏洞。任何人都可查看 AtmosConnect 的源代码，通过 authenticateBackdoorUser 逆向推算出密码。攻击者可借助该漏洞滥用 AmosConnect 任务管理器在远程系统上执行具有 SYSTEM 权限的命令。除了该后门，登录表单中的 SQL 注入漏洞也对该平台构成影响，攻击者可访问内部数据库存储的凭证。

参考链接：<https://www.easyaq.com/news/703213534.shtml?from=timeline&isappinstalled=0>

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：010-82991537