

信息安全漏洞周报

2017 年 10 月 16 日-2017 年 10 月 22 日

2017 年第 43 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**高**。

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 597 个，其中高危漏洞 114 个、中危漏洞 442 个、低危漏洞 41 个。漏洞平均分为 5.44。本周收录的漏洞中，涉及 0day 漏洞 190 个（占 32%），其中互联网上出现“Intelbras WRN 150 安全绕过漏洞、Joomla! Quiz Deluxe 组件 SQL 注入漏洞”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 635 个，与上周（818 个）环比下降 22%。

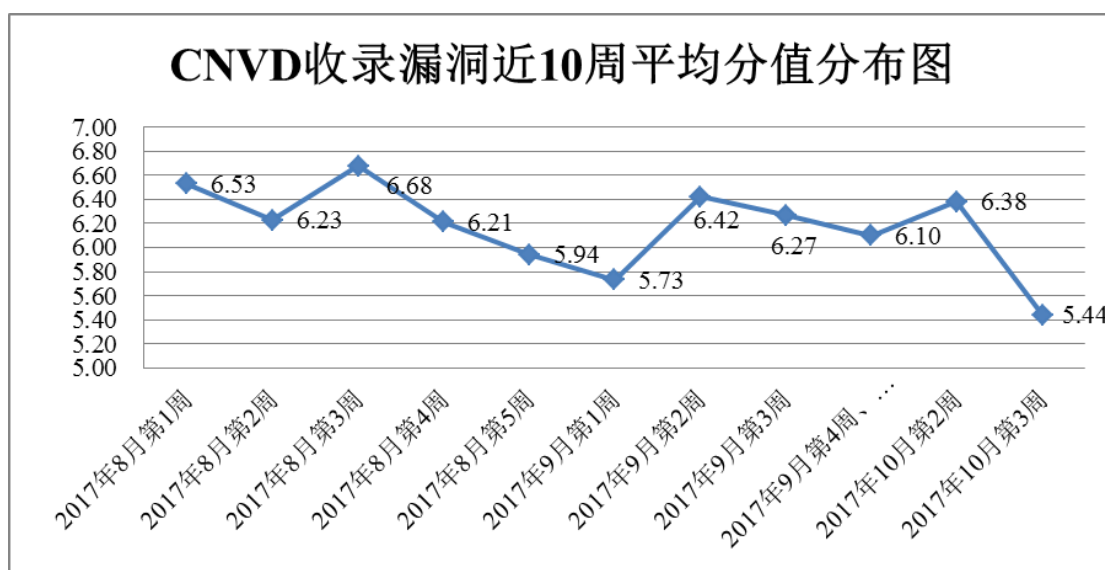


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，H3C、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。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、福建榕基软件股份有限公

司、广州万方计算机科技有限公司、湖南省金盾信息安全等级保护评估中心有限公司、江苏同袍信息科技有限公司、网信智安及其他个人白帽子向 CNVD 提交了 635 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
H3C	255	0
安天实验室	212	0
天融信	211	0
华为技术有限公司	199	0
恒安嘉新	189	0
网神	170	170
漏洞盒子	108	108
启明星辰	91	13
中国电信集团系统集成有 限责任公司	81	0
绿盟科技	75	0
杭州安恒信息技术有限公 司	50	0
厦门服云信息科技有限公 司	21	0
东软	2	2
知道创宇	1	1
深圳市鼎安天下信息科技 有限公司	18	18
四川虹微技术有限公司 (子午攻防实验室)	11	11
中新网络信息安全股份有 限公司	3	3
福建榕基软件股份有限公 司	3	3
广州万方计算机科技有限 公司	1	1
湖南省金盾信息安全等级 保护评估中心有限公司	1	1

江苏同袍信息科技有限公司	1	1
网信智安	1	1
CNCERT 新疆分中心	9	9
CNCERT 上海分中心	8	8
CNCERT 广东分中心	6	6
CNCERT 海南分中心	4	4
CNCERT 辽宁分中心	3	3
CNCERT 陕西分中心	2	2
CNCERT 西藏分中心	2	2
个人	268	268
报送总计	2006	635

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 597 个漏洞。其中应用程序漏洞 460 个，web 应用漏洞 60 个，操作系统漏洞 40 个，网络设备漏洞 30 个，数据库漏洞 6 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	460
web 应用漏洞	60
操作系统漏洞	40
网络设备漏洞	30
数据库漏洞	6
安全产品漏洞	1

表 2 漏洞按影响类型统计表

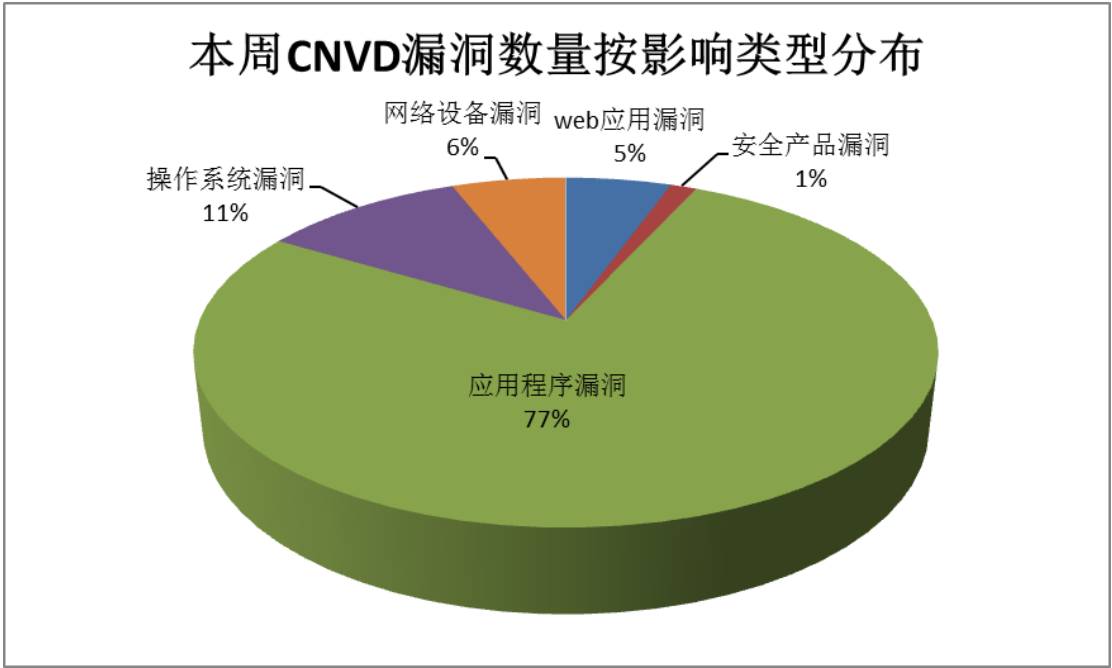


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Stdutility、Microsoft、IrfanView 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	Stdutility	67	11%
2	Microsoft	61	10%
3	IrfanView	28	5%
4	Oracle	24	4%
5	Kanboard	18	3%
6	IBM	14	2%
7	Huawei	13	2%
8	Intel	13	2%
9	Exiv2	10	2%
10	其他	349	59%

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 27 个电信行业漏洞，21 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，“fli4l HTTP header 注入漏洞、fli4l 任意代码执行漏洞、AVM FRITZ!Box 6810 LTE 和 FRITZ!Box 6840 LTE 代码注入漏洞、Kaspersky I

nternet Security for Android 安全绕过漏洞”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/>

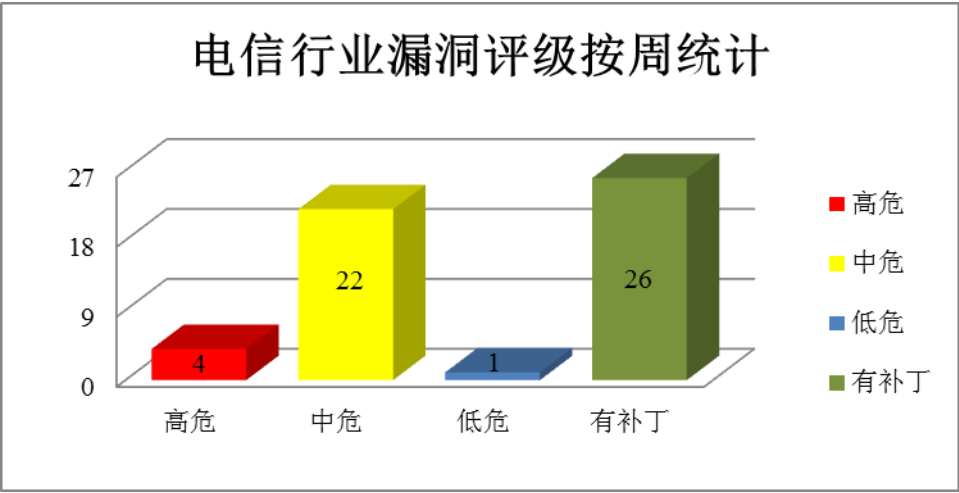


图 3 电信行业漏洞统计

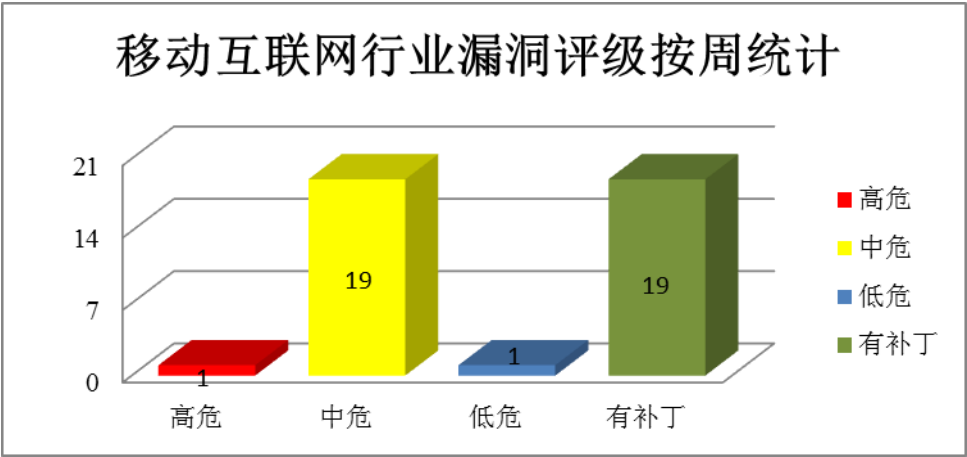


图 4 移动互联网行业漏洞统计

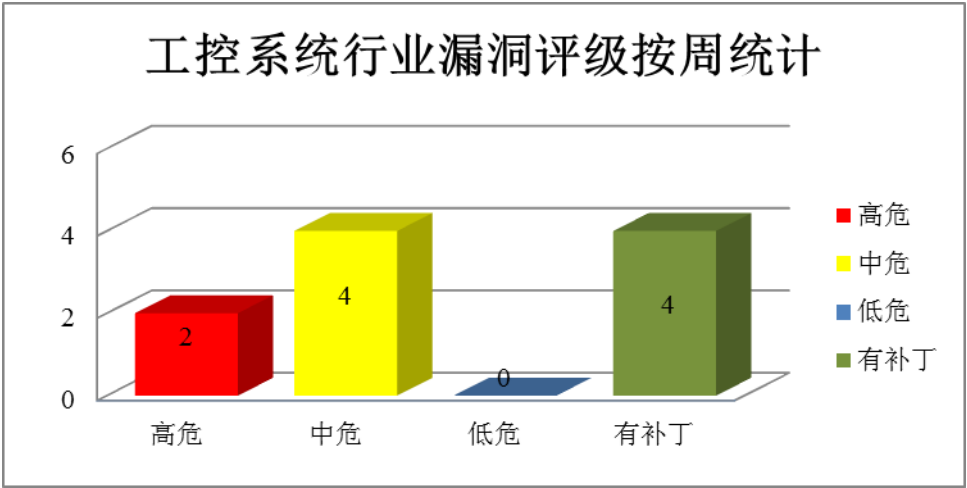


图 5 工控系统行业漏洞统计

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、Wi-Fi Alliance 产品安全漏洞

WPA（Wi-Fi Protected Access）是一种保护无线电脑网络（Wi-Fi）安全的系统。本周，该产品被披露存在密钥重装漏洞，攻击者可利用漏洞任意数据包解密和注入，TCP 连接劫持，HTTP 内容注入或单播和组寻址帧的重放。

CNVD 收录的相关漏洞包括：WPA2 无线网络 GTK 组密钥重装漏洞（CNVD-2017-30402、CNVD-2017-30403）、WPA2 无线网络 GTK 组密钥重装漏洞、WPA2 无线网络 GTK 组密钥重装漏洞、WPA2 无线网络 GTK 组密钥重装漏洞、WPA2 无线网络 GTK 组密钥重装漏洞、WPA2 无线网络 GTK 组密钥重装漏洞、WPA2 无线网络 GTK 组密钥重装漏洞、WPA2 无线网络 GTK 组密钥重装漏洞、WPA2 无线网络 GTK 组密钥重装漏洞。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-2017-30402>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30403>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30405>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30404>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30406>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30401>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30400>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30399>

2、Microsoft 产品安全漏洞

Microsoft Windows Server 2016 等都是美国微软公司发布的操作系统。Internet Explorer（IE）是其中的一个浏览器。Microsoft Edge 是内置于 Windows 10 版本中的网页浏览器。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：Microsoft Edge 脚本引擎远程内存破坏漏洞（CNVD-2017-30539、CNVD-2017-30540、CNVD-2017-30541、CNVD-2017-30542、CNVD-2017-30543）、Microsoft Internet Explorer Scripting 内存破坏漏洞、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2017-30134、CNVD-2017-30137）。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-2017-30539>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30540>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30541>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30542>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30543>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30131>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30134>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30137>

3、Oracle 产品安全漏洞

Oracle Hospitality Applications 是美国甲骨文公司的一套用于酒店管理的业务应用程序、服务器和存储解决方案。Hospitality Suite8 是其中的一个高级客户管理组件。本周，该产品被披露存在未明漏洞，攻击者可利用漏洞影响系统的机密性、完整性及可用性。

CNVD 收录的相关漏洞包括：Oracle Hospitality Suite8 存在未明漏洞（CNVD-2017-30879、CNVD-2017-30880、CNVD-2017-30881、CNVD-2017-30882、CNVD-2017-30883、CNVD-2017-30884、CNVD-2017-30885、CNVD-2017-30886）。其中，“Oracle Hospitality Suite8 存在未明漏洞（CNVD-2017-30880、CNVD-2017-30881）”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-2017-30879>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30880>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30881>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30882>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30883>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30884>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30885>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30886>

4、Huawei 产品安全漏洞

Huawei FusionSphere 和 FusionSphere OpenStack（FSO）都是华为公司的产品，前者是基于 OpenStack 框架开发的云操作系统产品，后者是 FusionSphere 在 ICT 场景中的云平台软件。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、提升权限或插入恶意程序等。

CNVD 收录的相关漏洞包括：Huawei FusionSphere OpenStack 鉴权不当漏洞、Huawei FusionSphere OpenStack 鉴权不当漏洞（CNVD-2017-30767）、Huawei FusionSphere OpenStack 路径校验漏洞、Huawei FusionSphere OpenStack 命令注入漏洞（CNVD-2017-30766、CNVD-2017-30901）、Huawei FusionSphere OpenStack 签名校验漏洞、Huawei FusionSphere OpenStack 权限提升漏洞、Huawei FusionSphere OpenStack 信息泄露漏洞。除“Huawei FusionSphere OpenStack 路径校验漏洞”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-2017-29734>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30067>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30068>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30069>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30072>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30073>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30074>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30075>

5、Progea Movicon SCADA/HMI 权限提升漏洞

Movicon 是由意大利自动化软件供应商 PROGEA 公司开发的(Scada/HMI)工业监控软件。本周, Progea 被披露存在权限提升漏洞, 本地用户可将任意代码插入到未引用的服务路径中, 并升级其权限。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-2017-30496>

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-2017-30243	xen 权限提升漏洞 (CNVD-2017-30243)	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-244.html
CNVD-2017-30246	xen 系统内存访问漏洞	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-241.html
CNVD-2017-30343	Sudo sudoers 插件设计漏洞	高	厂商已发布了漏洞修复程序, 请及时关注更新: https://www.sudo.ws/
CNVD-2017-30570	NoMachine for Mac OS X 和 Linux 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://www.nomachine.com/SU08O00185
CNVD-2017-30727	Netsweeper 认证绕过漏洞 (CNVD-2017-30727)	高	厂商已发布了漏洞修复程序, 请及时关注更新: http://www.netsweeper.com/
CNVD-2017-30729	Netsweeper 认证绕过漏洞 (CNVD-2017-30729)	高	厂商已发布了漏洞修复程序, 请及时关注更新: http://www.netsweeper.com/

CNVD-2017-30738	RubyGems 安全绕过漏（CNVD-2017-30738）	高	厂商已发布漏洞修复程序，请及时关注更新： http://securitytracker.com/id/1039249
CNVD-2017-30746	多款 ZOHO 产品路径遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://demo.servicedeskplus.com/
CNVD-2017-30747	Barracuda Load Balancer 硬编码弱凭据漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.barracuda.com/
CNVD-2017-30748	Barracuda Load Balancer 权限访问控制漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.barracuda.com/

表 4 部分重要高危漏洞列表

小结：本周，Wi-Fi Alliance 被披露存在密钥重装漏洞，攻击者可利用漏洞任意数据包解密和注入，TCP 连接劫持，HTTP 内容注入或单播和组寻址帧的重放。此外，Microsoft、Oracle、Huawei 多款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、提升权限或执行任意代码等。另外，Progea 被披露存在权限提升漏洞，本地用户可将任意代码插入到未引用的服务路径中，并升级其权限。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. WPA2 安全协议存在多个高危漏洞

近日，鲁汶大学的研究人员 Mathy Vanhoef 在 WPA2 协议中发现了严重的安全漏洞，这对无线网络的安全造成了极大的考验。攻击者可以利用 KRACK 攻击读取先前认为是安全的敏感信息，如信用卡号，密码，聊天信息，电子邮件，照片等。进行一些网络配置之后，它还可以注入和操作数据。建议大家近期多关注路由器控制面板里的检查更新，也可以去路由器厂商的网站看看有没有更新固件。

参考链接：<http://www.freebuf.com/news/150917.html>

2. Adobe ColdFusion 存在反序列化漏洞

Adobe ColdFusion 是一个动态 Web 服务器，其 CFML 是一种程序设计语言，类似现在的 JSP 里的 JSTL。Adobe ColdFusion 在开启“Remote Adobe LiveCycle Data Management access”功能的条件下会开启 rmi registry 服务。会在本地监听 1099 端口。可通过 RMI 协议向 Adobe ColdFusion 服务端发送精心构造的反序列化代码来触发漏洞。

参考链接：<https://mp.weixin.qq.com/s/I-IizZsXUAfmpZaWUcecXQ>

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