

信息安全漏洞周报

2016 年 09 月 26 日-2016 年 10 月 09 日

2016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**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 391 个，其中高危漏洞 181 个、中危漏洞 192 个、低危漏洞 18 个。漏洞平均分为 6.49。本周收录的漏洞中，涉及 0day 漏洞 65 个（占 17%）。其中互联网上出现“Joomla! Pay Plans Extension 'index.php' SQL 注入漏洞”、“OpenJPEG 远程代码执行漏洞”等零日代码攻击漏洞以及有可能出现大规模利用的“Tomcat 本地提权漏洞”，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 1517 个，与上周（892 个）环比增长 41%。

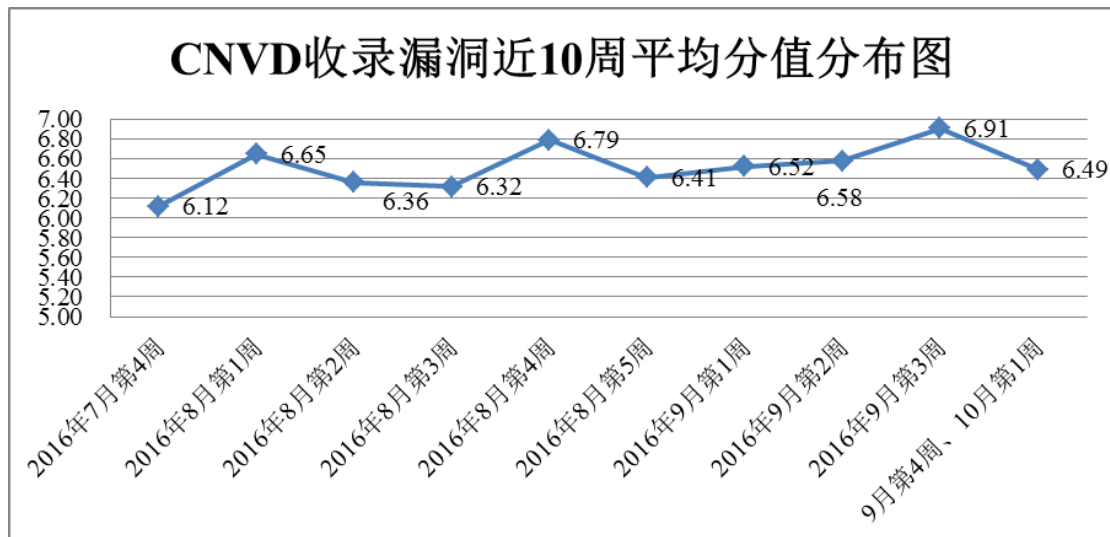


图 1 CNVD 收录漏洞近 10 周平均分分布图

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 391 个漏洞。报送情况如表 1 所示。其中，天融信、安天实验室、蓝盾信息安全技术有限公司、绿盟科技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\广州神月信息安全技术有限公司、广州圣辉信息技术有限公司、江苏君立华域信息安全技术有限公司、上海零盾网络科技有限公司、山石网科通信技术有限公司及其他个人白帽子向 CNVD 提交了 1517 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）	1313	1313
东软	229	0
天融信	198	0
安天实验室	157	0
蓝盾信息安全技术有限公司	145	0
绿盟科技	137	0
启明星辰	128	0
杭州安恒信息技术有限公司	113	41
恒安嘉新	90	0
H3C	68	0
中国电信集团系统集成有限责任公司	39	0
漏洞盒子	82	82
广西鑫瀚科技有限公司	19	19
广州神月信息安全技术有限公司	8	8
广州圣辉信息技术有限公司	4	4
江苏君立华域信息安全技术有限公司	2	2
上海零盾网络科技有限公司	1	1
山石网科通信技术有限公司	1	1
CNCERT 天津分中心	2	2
CNCERT 陕西分中心	1	1

CNCERT 宁夏分中心	1	1
个人	42	42
报送总计	2780	1517
录入总计	391（去重）	1517

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 391 个漏洞。其中应用程序漏洞 204 个，web 应用漏洞 84 个，操作系统漏洞 66 个，网络设备漏洞 24 个，安全产品漏洞 10 个，数据库漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	204
web 应用漏洞	84
操作系统漏洞	66
网络设备漏洞	24
安全产品漏洞	10
数据库漏洞	3

表 2 漏洞按影响类型统计表

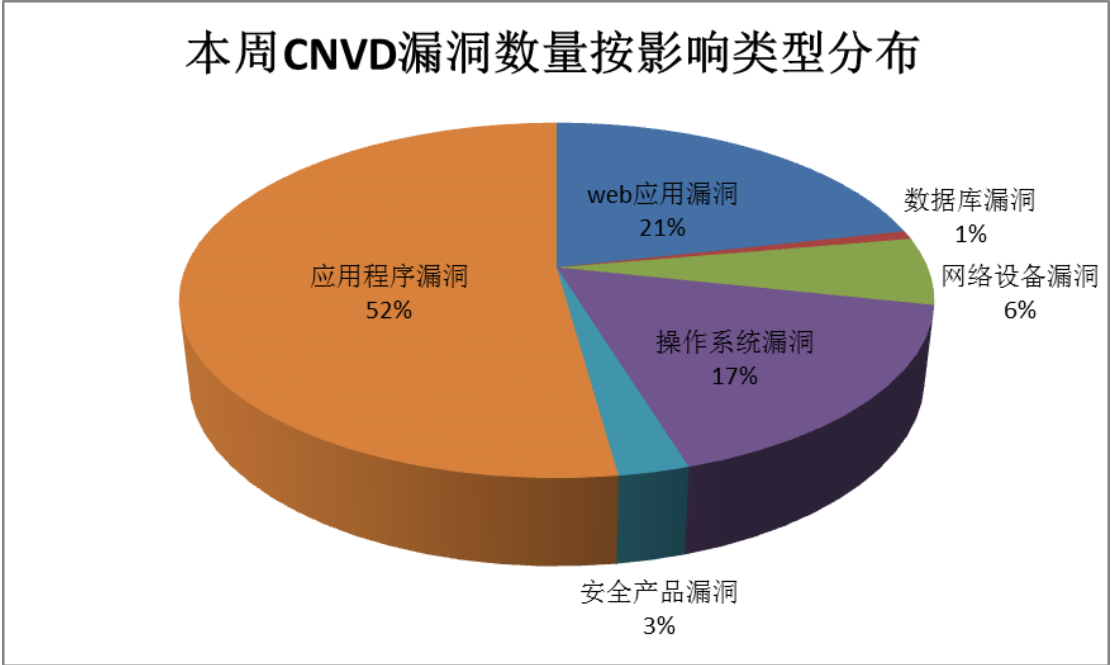


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、IBM、Cisco 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	65	17%
2	IBM	32	8%
3	Cisco	27	7%
4	ImageMagick	26	7%
5	Mozilla	18	5%
6	Huawei	10	3%
7	WordPress	10	3%
8	OpenSSL	8	2%
9	Joomla!	6	2%
10	其他	189	46%

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 21 个电信行业漏洞，45 个移动互联网行业漏洞，2 个工控系统行业漏洞（如下图所示）。其中，“Apple iOS/Safari/tvOS WebKit 内存破坏漏洞（CNVD-2016-08298、CNVD-2016-08299、CNVD-2016-08300、CNVD-2016-08301）、Cisco IOS and IOS XE Software 拒绝服务漏洞（CNVD-2016-08388、CNVD-2016-08389、CNVD-2016-08394、CNVD-2016-08395、CNVD-2016-08397）、HP Network Automation Java Deserialization 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/>

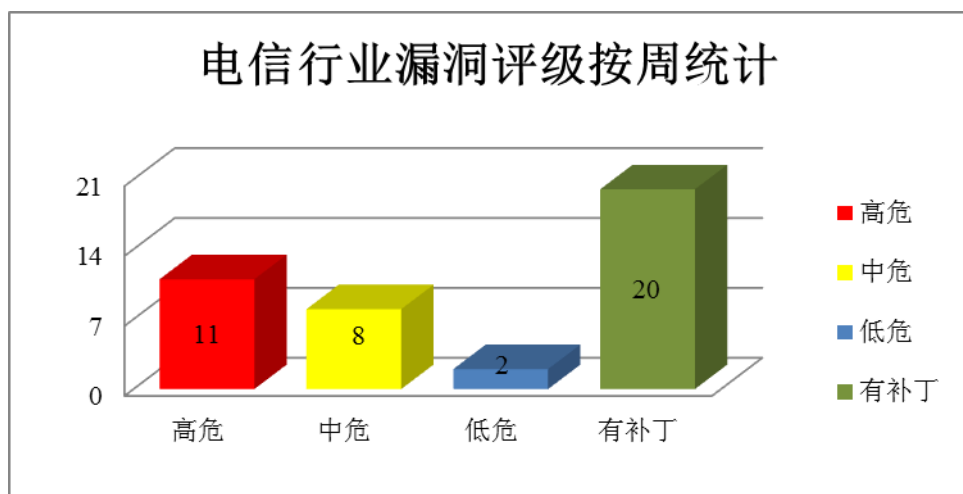


图 3 电信行业漏洞统计

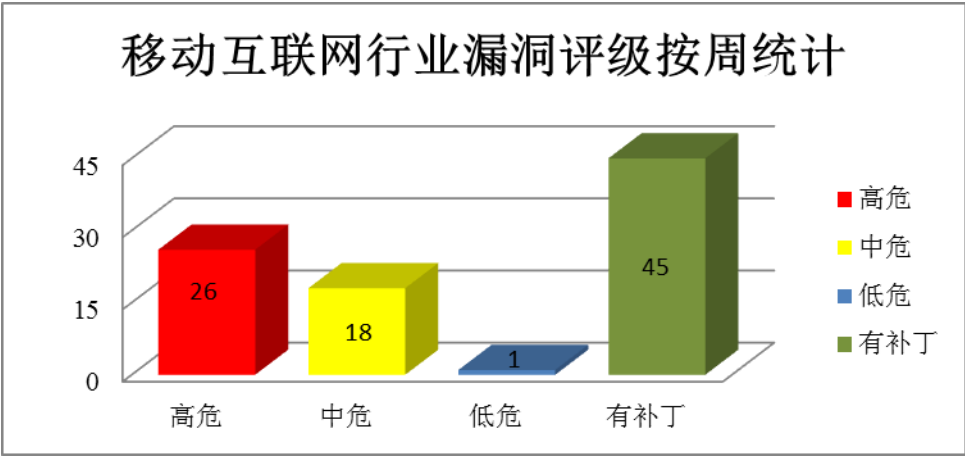


图 4 移动互联网行业漏洞统计

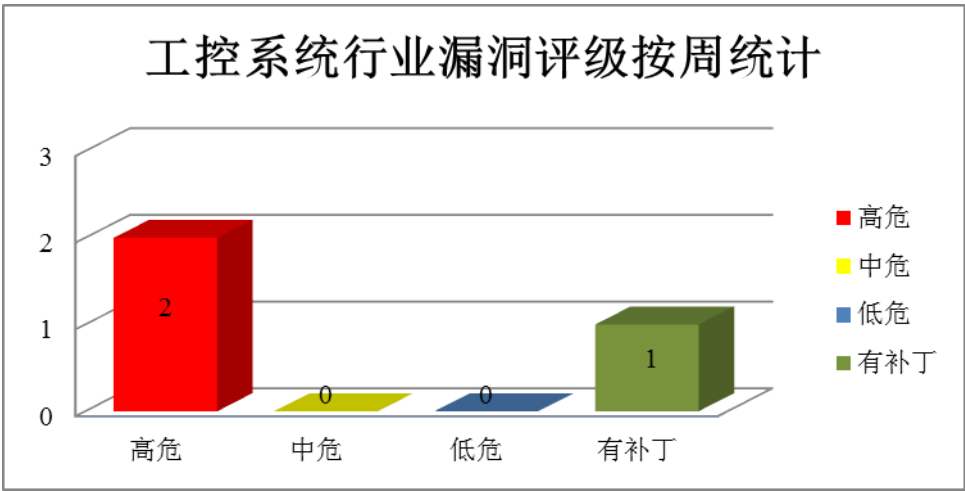


图 5 工控系统行业漏洞统计



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 OS X 是美国苹果（Apple）公司为 Mac 计算机所开发的一套专用操作系统。Kernel 是其中的一个内核组件。Apple iOS 是移动设备所开发的一套操作系统。WebKit 是 KDE、苹果（Apple）、谷歌（Google）等公司共同开发的一套开源 Web 浏览器引擎。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用该漏洞执行任意代码或造成拒绝服务（内存破坏）。

CNVD 收录的相关漏洞包括：Apple iOS WebKit 内存破坏漏洞（CNVD-2016-08099、CNVD-2016-08098、CNVD-2016-08097）、Apple OS X Kernel 内存破坏漏洞（CNVD-2016-08117、CNVD-2016-08116、CNVD-2016-08115、CNVD-2016-08114、CNVD-2016-08113）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-2016-08099>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08098>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08097>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08117>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08116>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08115>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08114>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08113>

2、IBM 产品安全漏洞

IBM Security Access Manager 是美国 IBM 公司的一款安全访问管理器。IBM Web Sphere Application Server (WAS) 是美国 IBM 公司开发并发行的一款应用服务器产品。IBM Tivoli Lightweight Infrastructure (又名 LWI) 是一个轻量级架构。IBM Spectrum Control 和 IBM Storage Insights 都是美国 IBM 公司的存储资源管理软件。IBM Tealeaf Customer Experience 是一套基于 SaaS 的网络和移动应用分析解决方案。IBM Security Guardium Database Activity Monitor 是美国 IBM 公司的一款数据库活动监控器产品。IBM DB2 是美国 IBM 公司的一套关系型数据库管理系统。本周，上述产品被披露存多个漏洞，攻击者可利用该漏洞获取提升的权限、上传任意文件或绕过安全限制等。

CNVD 收录的相关漏洞包括：IBM Security Access Manager 安全绕过漏洞 (CNVD-2016-08438)、IBM WebSphere Application Server 远程代码执行漏洞、IBM Tivoli Lightweight Infrastructure 目录遍历漏洞、IBM Spectrum Control 和 IBM Storage Insights 任意文件上传漏洞、IBM Tealeaf Customer Experience 暴力破解漏洞、IBM Tealeaf Customer Experience 安全绕过漏洞、IBM Security Guardium Database Activity Monitor 权限获取漏洞、多款 IBM DB2 产品本地提权漏洞等。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-2016-08438>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08260>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08286>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08135>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08077>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08076>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08075>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08086>

3、Cisco 产品安全漏洞

Cisco IOS 和 IOS XE 都是美国思科（Cisco）公司为其网络设备开发的操作系统。本周，上述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：Cisco IOS/IOS multicast 子系统拒绝服务漏洞（CNVD-2016-08398）、Cisco IOS/IOS multicast 子系统拒绝服务漏洞、Cisco IOS and IOS XE Software 拒绝服务漏洞（CNVD-2016-08397、CNVD-2016-08395、CNVD-2016-08394、CNVD-2016-08389、CNVD-2016-08388、CNVD-2016-08386）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-2016-08398>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08385>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08397>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08395>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08394>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08389>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08388>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08386>

4、ImageMagick 产品安全漏洞

ImageMagick 是美国 ImageMagick Studio 公司的一套开源的图象处理软件。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：ImageMagick 堆缓冲区溢出漏洞（CNVD-2016-08167、CNVD-2016-08166、CNVD-2016-08165、CNVD-2016-08164、CNVD-2016-08163、CNVD-2016-08162、CNVD-2016-08161、CNVD-2016-08160）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-2016-08167>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08166>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08165>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08164>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08163>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08162>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08161>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-08160>

5、Joomla! PayPlans Extension 'index.php' SQL 注入漏洞

Joomla!是一款开源的内容管理系统。本周，Joomla!被披露存在 SQL 注入漏洞。攻

击者可利用该漏洞访问或修改数据。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-2016-08068>

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-2016-08036	GraphicsMagick 堆缓冲区溢出漏洞（CNVD-2016-08036）	高	用户可联系供应商获得补丁信息： http://www.graphicsmagick.org/index.html
CNVD-2016-08065	SAP Adaptive Server Enterprise SQL 注入漏洞（CNVD-2016-08065）	高	用户可联系供应商获得补丁信息： http://go.sap.com/product/data-mgmt/sybase-ase.html
CNVD-2016-08072	多款 EMC 产品任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://www.emc.com/
CNVD-2016-08082	Apache Tomcat 安全绕过漏洞（CNVD-2016-08082）	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://tomcat.apache.org/
CNVD-2016-08094	MyBB SQL 注入漏洞（CNVD-2016-08094）	高	目前该漏洞已在更新版本 1.8.7 中修复，参考链接如下： http://resources.mybb.com/downloads/mybb_1807.zip
CNVD-2016-08105	Exponent CMS 任意代码执行漏洞	高	目前厂商已经发布更新，详情请关注厂商主页或有关网址： http://seclists.org/oss-sec/2016/q3/594
CNVD-2016-08106	Exponent CMS 文件上传漏洞	高	目前厂商已经发布更新，详情请关注厂商主页或有关网址： http://seclists.org/oss-sec/2016/q3/594
CNVD-2016-08110	Kerio Control 内存破坏漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://www.kerio.com/products/kerio-control
CNVD-2016-08112	Kerio Control 跨站请求伪造漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://www.kerio.com/products/kerio-control

CNVD-2016-08190	Trend Micro Smart Protection Server 存在多个漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://success.trendmicro.com/solution/1114913
-----------------	--	---	--

表 4 部分重要高危漏洞列表

小结：本周，Apple 产品被披露存在内存破坏漏洞，攻击者可利用该漏洞执行任意代码或造成拒绝服务（内存破坏）。此外，IBM、Cisco、ImageMagick 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞获取提升的权限、上传任意文件或发起拒绝服务攻击等。另外，Joomla! 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞访问或修改数据。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

漏洞预警：Tomcat 曝本地提权漏洞（CVE-2016-1240 附 PoC）

Tomcat 是个运行在 Apache 上的应用服务器，支持运行 Servlet/JSP 应用程序的容器——可以将 Tomcat 看作是 Apache 的扩展，实际上 Tomcat 也可以独立于 Apache 运行。Debian 系统的 Linux 上管理员通常利用 apt-get 进行包管理，CVE-2016-1240 这一漏洞其问题出在 Tomcat 的 deb 包中，使 deb 包安装的 Tomcat 程序会自动为管理员安装一个启动脚本：/etc/init.d/tocat* 利用该脚本，可导致攻击者通过低权限的 Tomcat 用户获得系统 root 权限！本地攻击者，作为 tomcat 用户（比如说，通过 web 应用的漏洞）若将 catalina.out 修改为指向任意系统文件的链接，一旦 Tomcat init 脚本（ROOT 权限运行）在服务重启后再次打开 catalina.out 文件，攻击者就可获取 ROOT 权限。

参考链接：<http://www.freebuf.com/vuls/115862.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