漏洞编号:CVE-2021-30640

漏洞描述:

漏洞来源: 平台 NVD

链接 https://nvd.nist.gov/vuln/detail/CVE-2021-30640

漏洞披露时间: 07/12/2021

漏洞参考链接:

野外漏洞报告：

<https://avd.aliyun.com/detail?id=AVD-2021-30640>

这个是阿里云的一篇报告，但是关键信息都很模糊。关于这个漏洞的报告非常少见

漏洞类型: CWE-116

漏洞危害: 输出编码不正确或转义

漏洞严重性:

CVSS 3.x评分：6.5

CVSS 2.0 评分：5.8

漏洞影响的组件版本:

apache:tomcat 7.0.0-7.0.109; 8.5.0-8.5.66; 9.0.0-9.0.46; 10.0.0-10.0.6

oracle:communications\_diameter\_signaling\_router 8.0.0-8.5.0

oracle:tekelec\_platform\_distribution 7.4.0-7.7.1

漏洞修复的组件版本:

漏洞成因:

JNDI Realm所做的查询并不总是正确地转义参数。在有限的情况下，用户可以使用其用户名的变体进行身份验证绕过 LockOut Realm 提供的某些保护

漏洞位置:

test/org/apache/catalina/realm/TestJNDIRealmIntegration.java 第52~55行

test/org/apache/catalina/realm/TestJNDIRealmIntegration.java第61、62行

漏洞PoC：

目前找不到这个漏洞的Poc

漏洞补丁：

<https://github.com/apache/tomcat/commit/24dfb30076997b640e5123e92c4b8d7f206f609c>

https://github.com/apache/tomcat/commit/0a272b00aed57526dbfc8b881ab253c23c61f100

<https://github.com/apache/tomcat/commit/c9f21a2a7908c7c4ecd4f9bb495d3ee36a2bd822>

<https://github.com/apache/tomcat/commit/4e86b4ea0d1a9b00fa93971c31b93ad1bd49c7fe>

<https://github.com/apache/tomcat/commit/79580e7f70a07c083be07307376511bb864d5a7b>

<https://github.com/apache/tomcat/commit/d3407672774e372fae8b5898d55f85d16f22b972>

<https://github.com/apache/tomcat/commit/6a9129ac9bd06555ce04bb564a76fc3987311f38>

https://github.com/apache/tomcat/commit/ad22db641dcd61c2e8078f658fa709897b5da375

漏洞处置建议：