**漏洞报告**

漏洞编号: CVE-2021- 25640

漏洞描述:

在Apache Dubbo软件2.6.9到2.7.9版本中，parseURL的使用会导致绕过白名单的检测，从而会引发开放式重定向或者SSRF漏洞。

漏洞来源:

平台: CVE/NVD

链接: <https://nvd.nist.gov/vuln/detail/CVE-2021-25640>

漏洞披露时间: 06/01/2021

漏洞参考链接: N/A

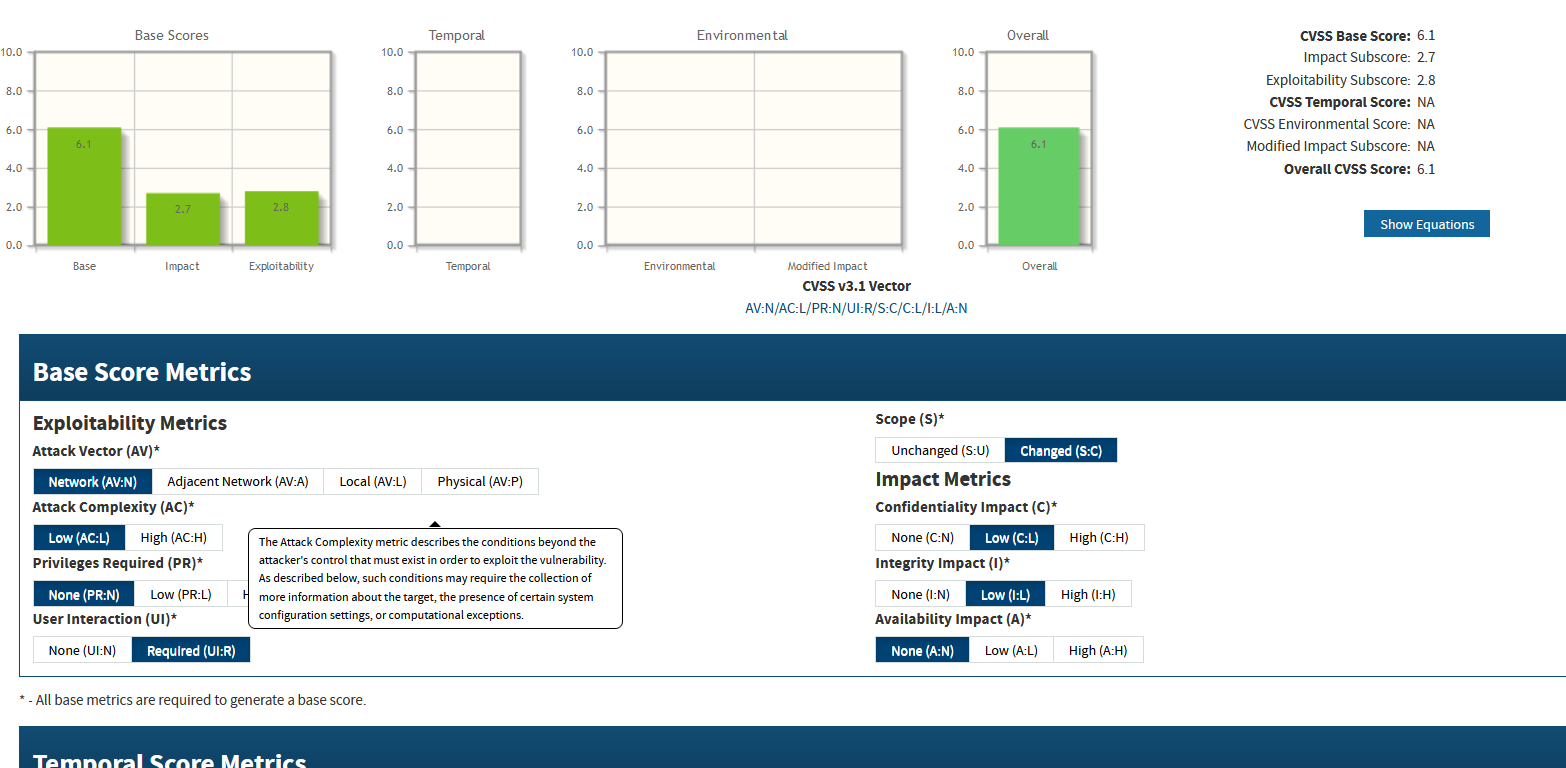
野外漏洞报告:

链接: <https://zhuanlan.zhihu.com/p/345902124>

漏洞类型: CWE-918

漏洞危害: 绕过白名单，可能会引发开放式重定向或者SSRF漏洞

CVSS评分: 6.1(已检验)



漏洞影响的组件版本:

Dubbo 2.7.0 到 2.7.9版本

Dubbo 2.6.0 到2.6.9版本

Dubbo 所有 2.5.x 版本 (不再被官方维护)

漏洞修复的组件版本:

Dubbo 2.6.9 2.7.9

漏洞成因:

参考链接: <https://zhuanlan.zhihu.com/p/345902124>中的对于Dubbo有关的内容

漏洞位置: 根据补丁推断出该漏洞应该在dubbo-dubbo-2.7.8\dubbo-common\src\main\java\org\apache\dubbo\common\utils\UrlUtils.java中parseURL函数3

漏洞PoC: N/A

备注：该漏洞的解决建议是将软件更新到2.7.10 +或者2.6.9 +，暂时没有发现相关的漏洞poc

漏洞补丁:

链接: <https://github.com/apache/dubbo/commit/b100a6d22b5cf051f76dad2b05aaf88e74e22154>

漏洞处置建议：

根据当前使用的版本将dubbo相应升级到2.7.10+或2.6.9+。

<https://cn.dubbo.apache.org/en/blog/2020/05/18/past-releases/>