知 ADWAN5.0承载网方案相关产品不涉及Apache Dubbo多个漏洞

ADWAN解决方案 田毓磊 2021-06-04 发表

漏洞相关信息

漏洞编号: CVE-2021-25641、CVE-2021-30181

漏洞名称: Apache Dubbo协议绕过漏洞/远程代码执行漏洞

产品型号及版本: SNA Center E1209、SeerEngine-WAN E6105H06、SeerAnalyzer E2101P10、License Server E1150

漏洞描述

1. Apache Dubbo协议绕过漏洞

由于Dubbo设置的serialization id存在被绕过风险, 攻击者通过伪造简单的serialization id, 绕过Dubbo审核机制导致未授权访问, 从而进行下一步的攻击。

2. Apache Dubbo远程代码执行漏洞

在版本2.6.9和2.7.9之间的Apache Dubbo支持脚本路由, 这使得客户能够将请求路由到正确的服务器。Dubbo使用ScriptEngine运行脚本来分析客户所使用的请求规则, 成功构造恶意脚本, 即可造成远程代码执行。

漏洞解决方案

SNA Center、SeerEngine-WAN、SeerAnalyzer、License Server产品不涉及Apache Dubbo多个漏洞

•