ADWAN5.0承载网方案相关产品不涉及WebLogic多个组件高危漏洞

ADWAN控制器 ADWAN解决方案 田晓磊 2021-07-24 发表

漏洞相关信息

漏洞编号： CVE-2021-2394、 CVE-2021-2397、 CVE-2021- 2382、 CVE-2021-2376、 CVE-2021-2378、 CVE-2015-0254、 CVE-2021-2403

漏洞名称： WebLogic多个组件高危漏洞

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

漏洞描述

一、漏洞描述：

Oracle官方发布了2021年7月的关键补丁程序更新，涉及旗下多款产品（Weblogic Server、 Database Server、 Java SE、 MySQL等）的 342 个漏洞。

此次修复的漏洞中包括 7 个和 Weblogic 相关的漏洞，这些漏洞无需身份 验证即可通过网络进行远程利用： CVE-2021-2394、 CVE-2021-2397、 CVE-2021- 2382、 CVE-2021-2376、 CVE-2021-2378、 CVE-2015-0254、 CVE-2021-2403。

安全专家建议受影响的版本尽快升级到最新版本， Weblogic 高危漏洞危害 极大，多年来一直是网络黑产最偏爱的漏洞攻击武器。

Oracle WebLogic Server是美国甲骨文（Oracle）公司的一款适用于云环境和传统环境的应用服务中间件， WebLogic 是用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用。

二、漏洞编号：

（1）CVE-2021-2394

该漏洞允许未经身份验证的攻击者通过 T3、 IIOP 访问网络来破坏Oracle WebLogic Server。成功攻击此漏洞可能会导致 Oracle WebLogic Server 被接管。

CVSS评分： 9.8，危害等级：严重

（2）CVE-2021-2397

该漏洞允许未经身份验证的攻击者通过 T3、 IIOP 访问网络来破坏Oracle WebLogic Server。成功攻击此漏洞可能会导致 Oracle WebLogic Server 被接管。

CVSS评分： 9.8，危害等级：严重

（3）CVE-2021-2382

该漏洞允许未经身份验证的攻击者通过 T3、 IIOP 访问网络来破坏 Oracle WebLogic Server。成功攻击此漏洞可能会导致 Oracle WebLogic Server 被接管。

CVSS评分： 9.8，危害等级：严重

（4）CVE-2021-2378

该漏洞允许未经身份验证的攻击者通过 T3、 IIOP 访问网络来破坏Oracle WebLogic Server。成功攻击此漏洞可导致未经授权导致Oracle WebLogic Server 挂起或频繁重复崩溃（完全DOS）。

CVSS评分： 7.5，危害等级：高危

（5）CVE-2021-2376

该漏洞允许未经身份验证的攻击者通过 T3、 IIOP 访问网络来破坏Oracle WebLogic Server。成功攻击此漏洞可导致未经授权导致Oracle WebLogic Server 挂起或频繁重复崩溃（完全 DOS）。

CVSS评分： 7.5，危害等级：高危

（6）CVE-2015-0254

该漏洞由第三方工具（Apache Standard Taglibs）引起。1.2.3版本之前的Apache Standard Taglibs允许远程攻击者执行任意代码或进行外部 xml 实体 (XXE) 攻击。

CVSS评分： 7.3，危害等级：高危

（7）CVE-2021-2403

该漏洞允许未经身份验证的攻击者通过 HTTP 访问网络来破坏 Oracle WebLogic Server。成功攻击此漏洞可能会导致对 Oracle WebLogic Server 可访问数据的子集进行未经授权的读取访问。

CVSS评分： 5.3，危害等级：中危

三、影响范围：

Weblogic Server 10.3.6.0.0

Weblogic Server 12.1.3.0.0

Weblogic Server 12.2.1.3.0

Weblogic Server 12.2.1.4.0

Weblogic Server 14.1.1.0.0

漏洞解决方案

SNA Center、SeerEngine-WAN、SeerAnalyzer、License Server产品不涉及WebLogic多个组件高危漏洞。