



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Exploited Vulnerability in Oracle Agile Product Lifecycle Management
Tracking #:432316536
Date:20-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Oracle has issued a critical security alert for an actively exploited vulnerability in its Oracle Agile Product Lifecycle Management (PLM) software, which could potentially allow remote exploitation without authentication.

TECHNICAL DETAILS:

Oracle has issued a critical security alert for a vulnerability identified as CVE-2024-21287 in its Oracle Agile Product Lifecycle Management (PLM) software, which could potentially allow remote exploitation without authentication. This vulnerability poses a significant risk as it could lead to file disclosure when successfully exploited. The vulnerability is remotely exploitable over the network without the need for a username or password and has been exploited in the wild.

Vulnerability Details:

- **CVE ID:** CVE-2024-21287
- **Vulnerability Type:** File Disclosure
- **Exploitation Vector:** Remote (Network-based)
- **Authentication:** Not required (can be exploited without credentials)
- **Affected Products and Versions:** Oracle Agile PLM Framework, version 9.3.6

RECOMMENDATIONS:

- Organizations using affected versions of Oracle Agile PLM should apply the security patches released by Oracle as soon as possible to mitigate the risk.
- Upgrade to Supported Versions: For customers using versions of Oracle Agile PLM that are no longer under Premier or Extended Support, Oracle recommends upgrading to supported releases. These releases will receive ongoing security updates and patches.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://www.oracle.com/security-alerts/alert-cve-2024-21287.html>