مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Exploited Vulnerability- Oracle WebLogic Server

Tracking #:432315936

Date:07-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Oracle WebLogic Server. Threat actors are actively exploiting this vulnerability to execute malicious code on affected systems.

TECHNICAL DETAILS:

A critical OS command injection vulnerability (CVE-2017-3506) affecting Oracle WebLogic Server is under active exploitation. This flaw could allow attackers to gain unauthorized access to vulnerable systems and potentially take complete control.

Vulnerability Details:

- **CVE-2017-3506**
- CVSS v3 score: 7.4 High
- A vulnerability in the Web Services subcomponent of Oracle WebLogic Server, a core component of Oracle Fusion Middleware, allows unauthenticated attackers with network access to inject arbitrary operating system commands through HTTP requests.
- A successful attack could grant the attacker unauthorized access to critical data, the ability to create, delete, or modify data on the server, and potentially complete control of the entire system.

Affected Products:

- Oracle WebLogic Server versions 10.3.6.0, 12.1.3.0, 12.2.1.0, 12.2.1.1, and 12.2.1.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Oracle.

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://nvd.nist.gov/vuln/detail/CVE-2017-3506