مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Exploited Vulnerability in Oracle WebLogic Server

Tracking #:432316691

Date:31-12-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in Oracle WebLogic Server has been disclosed, with a proof-of-concept (PoC) exploit now publicly available and is exploited in wild.

TECHNICAL DETAILS:

Vulnerability Description:
CVE-2024-21182 is a remote code execution (RCE) vulnerability affecting Oracle WebLogic Server versions 12.2.1.4.0 and 14.1.1.0.0. The flaw resides in the handling of the T3 and IIOP protocols, which are commonly enabled by default in WebLogic configurations. This easily exploitable flaw allows unauthenticated attackers to remotely compromise affected servers via the T3 and IIOP protocols, potentially leading to arbitrary code execution and full system compromise. This vulnerability poses a significant risk to organizations using WebLogic Server, especially given the public availability of the exploit.

Key Points:

- Exploitable without authentication via T3 and IIOP protocols
- CVSS score: 7.5 (High)
- PoC exploit publicly shared on GitHub
- Potential for unauthorized access to critical data and full system compromise
- Risk Level: High. The PoC exploit has been released, increasing the likelihood of active exploitation in the wild.
- Affected Versions:
  - Oracle WebLogic Server 12.2.1.4.0
  - Oracle WebLogic Server 14.1.1.0.0

RECOMMENDATIONS:

- Oracle is expected to release an official patch in the upcoming Critical Patch Update (CPU). Organizations are advised to monitor Oracle's official site for the patch release and apply it as soon as possible.
- Disable the T3 and IIOP protocols immediately if they are not required.
- Begin network monitoring to detect exploitation attempts.
- Implement a regular patch management schedule to ensure all Oracle WebLogic Server instances remain up to date with the latest security patches.
- Continue to review and harden your system configurations for additional protection.

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-2024-21182