Alert Bulletin

Bulletin N.: 2024-14
Publication Date: 05/06/2024
Subject: Alert 2024-14 Active Exploitation in Oracle WebLogic Server
Traffic Light Protocol (TLP): White

Affected Product(s):

Oracle WebLogic Server, a component of the **Oracle Fusion Middleware** suite.

- **Affected Versions:**
  - **3.6.0**
  - **1.3.0**
  - **2.1.0**
  - **2.1.1**
  - **2.1.2**

Description:

Recently, there has been an increase in active exploitation of the **CVE-2017-3506** vulnerability in **Oracle WebLogic** by criminal groups. This vulnerability, with a severity score of **7.4**, resides in a component of the **Oracle Fusion Middleware** suite. Exploiting this vulnerability allows unauthenticated attackers to inject operating system-level commands by modifying HTTP requests, leveraging the server's XML processing functionality.

Moreover, it is crucial to note that any successful exploitation could lead to the creation, modification, or deletion of existing data in **Oracle WebLogic**, and the attack could potentially spread throughout the network.

This vulnerability was discovered in **2017**, but there is currently concurrent exploitation observed by the **8220 Gang**, a Chinese group focused on **cryptojacking** (exploiting assets for cryptocurrency mining without consent). This resurgence may be due to many of these applications not being updated and possibly using a proof-of-concept exploit for this vulnerability. The **Cybersecurity and Infrastructure Security Agency (CISA)** of the United States has added it to its **Known Exploited Vulnerabilities (KEV)** database.

Oracle WebLogic is a widely used product, with approximately **5,600 servers** exposed to the Internet worldwide. In **Mexico**, there are multiple servers exposed online, and as part of internal applications, which, although may not be directly exposed to the Internet, could be exploited as part of an attacker's lateral

movement strategy within a network after gaining access.

Impact:

A malicious actor who can remotely access our **Oracle WebLogic Server** application could modify our local data and potentially extend the attack throughout the internal network, resulting in significant impact on the infrastructure.

Solution:

Update the **Oracle WebLogic** software to the latest versions that address this vulnerability.