Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 276 **10-6-2024**

Name: Oracle WebLogic Server OS Command Injection Flaw Actively Exploited

Threat Classification: Vulnerability

Affected Software / Area:

- Oracle WebLogic Server Versions:
  - 10.3.6.0
  - 12.1.3.0
  - 12.2.1.0
  - 12.2.1.1
  - 12.2.1.2

Summary:

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has reported active exploitation of a critical OS command injection vulnerability in Oracle WebLogic Server, identified as CVE-2017-3506 (CVSS score: 7.4). This flaw allows attackers to execute arbitrary code by sending specially crafted HTTP requests containing malicious XML documents. The cryptojacking group, 8220 Gang, has historically exploited this vulnerability to create botnets for cryptocurrency mining.

Severity	**High**
Attack Vector	**Remote Code Excuation**

Recommendations:

- It is recommended to Immediately apply latest patches, upgrades, workaround information.
    - https://www.oracle.com/security-alerts/cpuapr2024.html
- Regularly monitor systems for unusual activity that might indicate an attempt to exploit these vulnerabilities.
- Implement multi-factor authentication (MFA) to strengthen login security.
- Implement network segmentation to contain and isolate potential threats, limiting their impact on critical systems.
- Establish a proactive patch management process to ensure timely deployment of security updates for all software and systems.
- In case of any incident, please report to this office, through PTA CERT Portal and email.