UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00060

ORACLE WEBLOGIC UNDER ACTIVE ATTACK

DATE ISSUED: 2nd November 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Oracle WebLogic Servers that have not been updated are vulnerable to a Remote Code Execution (RCE) vulnerability that is currently under active attack and has a current CVSS rating of 9.8/10. CVE-2020-14882

BREAKDOWN

This popular platform for building and deploying application using Java EE has a flaw present in the console that is considered by Oracle to be low in complexity. The flaw requires no user interact, no specified privileges and can be carried out across simply through HTTP network access and using a simple GET request. The security patch was released in Oracle's mass October release last week and has now seen a surge in attackers actively seeking out this flaw using scanning techniques. SANS researcher Johannes B. Ulrich believes based on their observations all IPv4 addresses have been scanned and any servers may potentially be already compromised.

REMEDIATION STEPS

- Update any servers using Oracle WebLogic versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0 using the Oracle Security Centre link below
- Limit scanning capabilities across your network by implementing the correct policies to prevent unauthorized scanning
- Monitor network for any suspicious activity and address alerts in a timely manner
- As the attacks seem to stem from four particular IP addresses, block the following: 114.243.211.182, 139.162.33.228, 185.225.19.240 and 84.17.37.239

REFERENCES & RESOURCES

Threatpost https://threatpost.com/oracle-weblogic-server-rce-flaw-attack/160723/
Cyber Guidance Issue 55 https://cdn-cms.f-static.net/uploads/3505113/normal_5f97d06b4af5e.pdf
Oracle Security Centre https://www.oracle.com/security-alerts/cpuoct2020traditional.html