UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00055

ORACLE OCTOBER PATCHES TOTAL 402

DATE ISSUED: 27th October 2020

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Oracle's quarterly patch update across its family of software includes solutions to 402 vulnerabilities, 272 of which are subject to remote exploitation, meaning attackers do not even need credentials to access the system. Two of which, have the highest possible CVSS (Common Vulnerability Scoring System) rating of 10/10.

BREAKDOWN

The most pressing flaws can be found in the Oracle Healthcare Foundation analytics platform and may be remotely executed requiring no user interaction whatsoever. This vulnerability is listed as CVE-2020-1953 and affects versions 7.1.1, 7.2.0, 7.2.1 and 7.3.0. The other 10/10 CVSS flaw CVE-2020-14871 affects Oracle Solaris in the pluggable authentication module, also requiring no user credentials or interventions.

REMEDIATION STEPS

- 27 Oracle applications are affected by the patched with the largest groups listed below. These applications, if in use, should apply all patches immediately using the link supplied below:
    - Oracle Financial Services Applications (53)
    - Oracle MySQL (53)
    - Oracle Communications (52)
    - Oracle Fusion Middleware (46)
    - Oracle Retail Applications (28)
    - Oracle E-business Suite (27)
- Oracle does not recommend using work-around methods as this may disrupt the proper function of the applications

REFERENCES & RESOURCES

Oracle Security Centre	https://www.oracle.com/security-alerts/cpuoct2020traditional.html
Threatpost	https://threatpost.com/oracle-october-patch-update/160407/
Tenable:	https://www.tenable.com/blog/oracle-critical-patch-update-for-october-2020-addresses-402-security-updates