CYBER GUIDANCE ISSUE 00214

ORACLE QUARTERLY UPDATE

DATE ISSUED: 26th October 2021

IMPACT	LOW	MEDIUM	HIGH

EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Oracle's quarterly update has seen 36 critical vulnerabilities patched, with a grand total of 419 vulnerabilities remediated across a vast range of products across Oracle native and third-party components.

BREAKDOWN

231 CVE's are addressed in the latest round of updates across 28 product families. Four families that are not included in this round of updates are Oracle Global Lifecycle Management, Oracle NoSQL Database, Oracle Spatial Studio, and Oracle SQL Developer. However, there are third-party patches included as part of its CPU release. The highest rated vulnerability is tracked as CVE-2021-35652 affecting Oracle Essbase which is a business analytics solution. Several of the vulnerabilities disclosed allow for Remote Code Execution (RCE). This is the final quarterly update for 2021.

REMEDIATION STEPS

- Check vulnerabilities in the resources provided below and apply security updates to bring those affected products in your environment. It is recommended you test updates in a non-production environment before deploying them to your live systems.
- Where a patch is not able to be applied immediately a workaround/mitigations suggestion from Oracle is available to block network protocols required for an attack – see resource below.
- Run all software as a non-privileged user to reduce risk of lateral movement in the event an account is compromised and ensure access to systems are on a need-to-know, least privilege basis.
- Educate users on the dangers of visiting untrusted websites and phishing/social engineering emails and how to deal with these in your organisation.

REFERENCES & RESOURCES

Oracle	https://www.oracle.com/security-alerts/cpuoct2021.html
	https://login.oracle.com/mysso/signon.jsp
Tenable	https://www.tenable.com/blog/oracle-october-2021-critical-patch-update-addresses-231-cves
CIS Advisory	