Security Advisory 2022-006

Critical Vulnerabilities in Multiple Oracle Products

January 20, 2022 — v1.0

TLP:WHITE

History:

• 20/01/2022 — v1.0 – Initial publication

Summary

On January 18th, Oracle released their quarterly Critical Patch Update advisory, a collection of patches that addresses hundreds of critical security flaws, affecting several of their products [1]. Many of these vulnerabilities may be remotely exploited without the need for user credentials. It is therefore highly recommended to apply the security patches without delay.

Technical Details

The January 2022 Critical Patch Update contains 497 security patches, many of which tackle critical vulnerabilities that are easily exploitable and can lead to system takeover, Denial of Service (DOS), and unauthorised creation, deletion or modification access to critical data [2].

Affected Products

The following Oracle Family products are affected. For further details (e.g., affected versions), please consult Oracle’s official page [1, 2]:

• Oracle Database Server
• Oracle Airlines Data Model
• Oracle Big Data Graph
• Oracle Communications Data Model
• Oracle Essbase
• Oracle GoldenGate
• Oracle Graph Server and Client
• Oracle NoSQL Database
• Oracle REST Data Services
• Oracle Secure Backup
• Oracle Spatial Studio
• Oracle TimesTen In-Memory Database
• Oracle Commerce
• Oracle Communications Applications
Recommendations

It is recommended to apply the patches for all affected products as soon as possible.

References