Security Advisory 2020-004

Critical Vulnerabilities in Multiple Oracle Products

January 15, 2020 — v1.0

TLP:WHITE

History:

• 15/01/2020 — v1.0 – Initial publication

Summary

Oracle has published an advisory about hundreds of critical vulnerabilities are affecting several of its products [1]. Many of the vulnerabilities can be remotely exploited without authentication and without user interaction. Expedient patching of the affected products is highly recommended.

Technical Details

The January 2020 Oracle Critical Patch Update contains 334 security patches for multiples products [1]. These patches are addressing various risks such as remote code execution, denial of service, system takeover, sensible data accessing and modification [2].

Affected products

The following product families from Oracle are affected. For details of the affected versions, please consult [1, 2]:

• Enterprise Manager
• Hyperion
• Identity Manager
• Instantis EnterpriseTrack
• JD Edwards EnterpriseOne
• MySQL
• Oracle Agile
• Oracle Application Testing Suite
• Oracle AutoVue
• Oracle Banking
• Oracle Big Data Discovery
• Oracle Business Intelligence Enterprise Edition
• Oracle Clinical
• Oracle Coherence
• Oracle Communications
• Oracle Database Server
• Oracle Demantra Demand Management
• Oracle E-Business Suite
• Oracle Endeca Information Discovery
• Oracle Enterprise
• Oracle Financial Services
• Oracle FLEXCUBE
• Oracle GraalVM Enterprise Edition
• Oracle Health Sciences Data Management Workbench
• Oracle Healthcare Master Person Index
• Oracle Hospitality
• Oracle HTTP Server
• Oracle iLearning
• Oracle Java SE
• Oracle Outside In Technology
• Oracle Real-Time Scheduler
• Oracle Reports Developer
• Oracle Retail
• Oracle Secure Global Desktop
• Oracle Security Service
• Oracle Solaris
• Oracle Tuxedo
• Oracle Utilities
• Oracle VM Server for SPARC
• Oracle VM VirtualBox
• Oracle WebCenter Sites
• Oracle WebLogic Server
• PeopleSoft
• Primavera
• Siebel Applications
• Sun ZFS Storage Appliance Kit
• Tape Library ACSLS

Recommendations

It is recommended to apply the patches from Oracle for all affected products.

References