Advisory Alert

Alert Number: AAA20220720 **Date:** July 20, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Oracle	**Critical**	**Multiple Vulnerabilities**
IBM	**Medium**	**Multiple Vulnerabilities**

Description

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released monthly security patch updates addressing multiple vulnerabilities that exists in their products. Oracle highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpujul2022.html

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22477, CVE-2021-29755, CVE-2022-22424)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their IBM QRadar and IBM WebSphere Application Server product. **CVE-2022-22477** – Due to a flaw that exists in IBM WebSphere Application Server it is vulnerable to cross-site scripting which allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **CVE-2021-29755** – IBM Qradar SIEM is vulnerable since it does not preform proper certificate validation for some inter-host communications. **CVE-2022-22424** - IBM QRadar is vulnerable since it could allow a local user to obtain sensitive information from the TLS key file due to incorrect file permissions. IBM highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM WebSphere Application Server 9.0 IBM WebSphere Application Server 8.5 IBM QRadar SIEM 7.3.0 - 7.3.3 Fix Pack 11 IBM QRadar SIEM 7.4.0 - 7.4.3 Fix Pack 5 IBM QRadar SIEM 7.5.0 - 7.5.0 Update Pack 1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6603417 https://www.ibm.com/support/pages/node/6605431 https://www.ibm.com/support/pages/node/6605433

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.