Advisory Alert

Alert Number: AAA20220615 **Date:** June 15, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Citrix	**Critical**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities
Intel	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-27511, CVE-2022-27512)
Description	Citrix has released security updates addressing multiple vulnerabilities that exists in the Citrix Application Delivery Management (Citrix ADM) platform. **CVE-2022-27511** – Due to this flaw an unauthenticated remote attacker can change the admin password by corrupting the system. **CVE-2022-27512** – Due to this flaw an attacker can temporarily disrupt the ADM license service Citrix highly recommends to apply necessary workarounds at earliest to avoid issues
Affected Products	Citrix ADM 13.1 before 13.1-21.53 Citrix ADM 13.0 before 13.0-85.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX460016/citrix-application-delivery-management-security-bulletin-for-cve202227511-and-cve202227512

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-21496, CVE-2022-21299)
Description	IBM has released patch updates to address multiple flaws in the IBM SDK, Java Technology Edition that is used in the IBM WebSphere Application Server and IBM WebSphere Application Server Liberty. **CVE-2022-21496** - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE allows unauthorized attacker with network access to perform in unauthorized update, insert, or delete operations to some of the accessible data on Oracle Java SE and Oracle GraalVM Enterprise Edition. **CVE-2022-21299** – Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE allows unauthorized attacker with network access to cause a partial denial of service (partial DOS) attack. IBM highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	WebSphere Application Server Liberty Continuous Delivery WebSphere Application Server v9.0 WebSphere Application Server v8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-ibm-java-sdk-affect-ibm-websphere-application-server-and-ibm-websphere-application-server-liberty-due-to-april-2022-cpu-plus-deferred-cve-2022-2129/

Affected Product	**Intel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-21123, CVE-2022-21125, CVE-2022-21127, CVE-2022-21166, CVE-2022-21180)
Description	Intel released firmware updates to address multiple vulnerabilities that exist in their intel processors. Exploitation of this vulnerabilities could allow denial of service in certain virtualized environments and information disclosure Intel highly recommends to apply these firmware updates at earliest to avoid issues
Affected Products	Multiple intel processors
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00645.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00615.html

Disclaimer

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