Advisory Alert

Alert Number: AAA20220624 **Date:** June 24, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High, Medium**	Multiple Vulnerabilities
Citrix	**Medium**	Privileged Code Execution Vulnerability

Description

Affected Product	**IBM**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22390, CVE-2022-25313, CVE-2022-25236, CVE-2022-25314, CVE-2022-25315, CVE-2022-25235, CVE-2022-22389)
Description	IBM has released patch updates addressing multiple vulnerabilities that exists in IBM DB2 products. Successful exploitation of these vulnerabilities could cause information disclosure, denial of service and arbitrary code execution. IBM highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	IBM Db2 V9.7, V10.1, V10.5, V11.1, and V11.5 server editions on all platforms.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6597993 https://www.ibm.com/support/pages/node/6597637 https://www.ibm.com/support/pages/node/6598047

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Privileged Code Execution Vulnerability (CVE-2022-26362)
Description	Citrix has released Security Update addressing a flaw in the Citrix Hypervisor that could allow privileged code in a PV guest VM to compromise the host. Citrix highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Citrix XenServer 7.1 CU2 LTSR: CTX459953 Citrix Hypervisor 8.2 CU1 LTSR: CTX459954
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX460064/citrix-hypervisor-security-update

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.