Advisory Alert

Alert Number: AAA20210806 **Date:** August 6, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Multiple Vulnerabilities
VMWare	**High**	Multiple Vulnerabilities

Description

Affected Product	IBM
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-29703, CVE-2021-29777)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-29703 – Due to this flaw an attacker could execute a specially crafted SELECT statement and cause the IBM Db2 server to terminate abnormally CVE-2021-29777 - Using this flaw under special circumstances an authenticated user could cause a denial of service when a table is dropped while being accessed in another session. IBM highly recommends to apply necessary security fixes to avoid issues.
Affected Products	All fix pack levels of IBM Db2 V9.7, V10.1, V10.5, V11.1, and V11.5 server editions on all platforms are affected.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6466371 https://www.ibm.com/support/pages/node/6466373

Affected Product	VMWare
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22002, CVE-2021-22003)
Description	VMWare has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-22002 - Due to this flaw a malicious actor with network access to port 443 could tamper with host headers to facilitate access to the /cfg web app and could access /cfg diagnostic endpoints without authentication. CVE-2021-22003 - Using this flaw a malicious actor with network access to port 7443 may attempt user enumeration or brute force the login endpoint and the account lockout policy configuration and password complexity of the target account can decrease the possibility of attack. VMWare highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	VMware Workspace One Access (Access) VMware Identity Manager (vIDM) VMware vRealize Automation (vRA) VMware Cloud Foundation vRealize Suite Lifecycle Manager
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0016.html

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.