Advisory Alert

Alert Number: AAA20201120 **Date:** November 20, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM DB2	**High**	Arbitrary code execute
VMware	**High**	Multiple vulnerabilities

Description

Affected Product	**IBM DB2**
Severity	**High**
Affected Vulnerability	Arbitrary code execute (CVE-2020-4739)
Description	IBM DB2 Accessories Suite for Linux, UNIX, and Windows DB2 for Linux, UNIX, and Windows (includes DB2 Connect Server) could allow a local authenticated attacker to execute arbitrary code on the system caused by DLL search order hijacking vulnerability in Microsoft Windows client. Specially crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system.
Affected Products	IBM Db2 V9.7, V10.1, V10.5, V11.1, V11.5 editions on Windows are affected
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6370023

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2020-3984, CVE-2020-3985, CVE-2020-4000, CVE-2020-4001, CVE-2020-4002 ,CVE-2020-4003)
Description	Multiple vulnerabilities in SD-WAN were privately reported to VMware. Patches and workarounds are available to remediate or workaround this vulnerability in affected VMware products. VMware-hosted SD-WAN have been patched for these issues. **CVE-2020-3984 -** Does not apply correct input validation which allows for SQL-injection. exploit a vulnerable API call using specially crafted SQL queries which may lead to unauthorized data access **CVE-2020-3985 -** Allows access to set arbitrary authorization levels leading to a privilege escalation issue. An authenticated user may exploit an application weakness and call a vulnerable API to elevate their privileges. **CVE-2020-4000 -** Allows for executing files through directory traversal. An authenticated user is able to traversal directories which may lead to code execution of files**.** **CVE-2020-4001 -** SD-WAN Orchestrator ships with default passwords for predefined accounts which may lead to to a Pass-the-Hash attack. **CVE-2020-4002 -** The SD-WAN Orchestrator handles system parameters in an insecure way. An authenticated SD-WAN Orchestrator user with high privileges may be able to execute arbitrary code on the underlying operating system. **CVE-2020-4003 -** This vulnerable to SQL-injection attacks allowing for potential information disclosure. An authenticated SD-WAN Orchestrator user may inject code into SQL queries. Which may lead to information disclosure.
Affected Products	VMware SD-WAN Orchestrator
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2020-0025.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.