TLP: WHITE

Advisory Alert

Alert Number: AAA20230201 **Date:** February 1, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Arbitrary code execution Vulnerability
IBM	**High**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
VMware	**Medium**	CSRF bypass Vulnerability
Ubuntu	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22558, CVE-2021-33117, CVE-2021-0154, CVE-2021-0153, CVE-2021-33123, CVE-2021-0190, CVE-2021-33122, CVE-2021-0189, CVE-2021-33124, CVE-2021-33103, CVE-2021-0159, CVE-2021-0188, CVE-2021-0155, CVE-2022-0004, CVE-2022-0005, CVE-2022-21131, CVE-2022-21136, CVE-2022-21123, CVE-2022-21125, CVE-2022-21127, CVE-2022-21166, CVE-2022-21233, CVE-2022-26074, CVE-2022-33060, CVE-2021-26316, CVE-2021-26398, CVE-2021-39298, CVE-2021-26402, CVE-2021-26353, CVE-2021-26355, CVE-2023-20529, CVE-2023-20530, CVE-2023-20531, CVE-2022-23813, CVE-2022-23814, CVE-2021-26396, CVE-2021-46779, CVE-2021-46791, CVE-2021-26328, CVE-2021-26407, CVE-2021-26409, CVE-2021-46768, CVE-2021-46767, CVE-2023-20522, CVE-2023-20523, CVE-2021-26404, CVE-2023-20525, CVE-2023-20527, CVE-2023-20528, CVE-2023-20532, CVE-2021-26403, CVE-2021-26343, CVE-2022-34377, CVE-2022-34376, CVE-2022-34406, CVE-2022-34407, CVE-2022-34408, CVE-2022-34409, CVE-2022-34410, CVE-2022-34411, CVE-2022-34412, CVE-2022-34413, CVE-2022-34414, CVE-2022-34415, CVE-2022-34416, CVE-2022-34417, CVE-2022-34418, CVE-2022-34419, CVE-2022-34420, CVE-2022-34421, CVE-2022-34422, CVE-2022-34423, CVE-2022-31680, CVE-2022-31681, CVE-2022-22982, CVE-2021-46827, CVE-2022-42889, CVE-2022-34435, CVE-2022-20824, CVE-2022-2601, CVE-2022-3775)
Description	Dell has released a security update addressing multiple vulnerabilities in Dell PowerFlex. If exploited these vulnerabilities could cause Information disclosure, privilege escalation and denial of service. Dell highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PowerFlex Rack RCM versions before 3.3.12.1, 3.4.7.1, 3.5.7.1, 3.6.3.1, 3.7.1.0 PowerFlex Appliance Versions before Intelligent_Catalog_38_363_01_r8, Intelligent_Catalog_38_357_01_r8, Intelligent_Catalog_40.371.00_r30
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000208056/dsa-2022-025-dell-emc-powerflex-rack-security-update-for-multiple-third-party-component-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000208055/dsa-2023-026-dell-emc-powerflex-appliance-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary code execution Vulnerability (CVE-2022-37601)
Description	IBM has released a Security Update addressing an Arbitrary code execution vulnerability that exist in IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data. Due to a prototype pollution flaw in the parseQuery function in parseQuery.js. of webpack loader-utils. A remote attacker could execute arbitrary code or cause a denial of service condition on the system by adding or modifying properties of Object.prototype using a __proto__ or constructor payload. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data • v3.5 through refresh 10 • v4.0 through refresh 9 • v4.5 through refresh 3 • v4.6 through refresh 1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6890703

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37599, CVE-2022-37603, CVE-2023-23477)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products **CVE-2022-37599** - A regular expression denial of service (ReDoS) flaw exist in interpolateName.js script of loader-utils in IBM Db2. A remote attacker could exploit this flaw by sending specially-crafted regex input. **CVE-2022-37603** - A regular expression denial of service (ReDoS) flaw exist in interpolateName.js script of webpack loader-utils in IBM Db2. A remote attacker could exploit this flaw by sending specially-crafted regex input using the url variable. **CVE-2023-23477**- IBM WebSphere Application Server traditional could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data • v3.5 through refresh 10 • v4.0 through refresh 9 • v4.5 through refresh 3 • v4.6 through refresh 1 IBM WebSphere Application Server 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6890703 https://www.ibm.com/support/pages/node/6891111

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2015-9251, CVE-2016-10735, CVE-2017-18214, CVE-2018-14040, CVE-2018-14041, CVE-2018-14042, CVE-2019-8331, CVE-2019-11358, CVE-2020-11022, CVE-2020-11023, CVE-2022-3143, CVE-2022-40149, CVE-2022-40150, CVE-2022-40152, CVE-2022-42003, CVE-2022-42004, CVE-2022-45047, CVE-2022-45693, CVE-2022-46364)
Description	Redhat has released Security Updates addressing Multiple Vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Cross-site scripting, Untrusted code execution, stackoverflow and memory exhaustion. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:0556 https://access.redhat.com/errata/RHSA-2023:0554

Affected Product	**VMware**
Severity	**Medium**
Affected Vulnerability	CSRF bypass vulnerability (CVE-2023-20856)
Description	VMware has released Security Updates addressing a CSRF bypass vulnerability that exist in VMware vRealize Operations (vROps). Due to the vulnerability a malicious user could execute actions on the platform on behalf of the authenticated victim user. VMware recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	VMware vRealize Operations (vROps) 8.6.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0002.html

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-36760, CVE-2006-20001, CVE-2022-47024, CVE-2023-0049, CVE-2023-0054, CVE-2023-0288, CVE-2023-0433)
Description	Ubuntu has released Security Updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to denial of service, arbitrary code execution and HTTP Request Smuggling attack. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5834-1 https://ubuntu.com/security/notices/USN-5836-1

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.