Advisory Alert

Alert Number: AAA20220421 **Date:** April 21, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Drupal	**Critical**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities

Description

Affected Product	IBM
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-3807, CVE-2021-3918, CVE-2021-32803, CVE-2021-32804, CVE-2021-27290, CVE-2021-23362, CVE-2021-23343, CVE-2021-22940, CVE-2021-22939, CVE-2021-22931, CVE-2021-22930, CVE-2021-22918, CVE-2021-3672, CVE-2020-28469, CVE-2021-33502, CVE-2022-23852, CVE-2022-23990)
Description	IBM has released Security Updates addressing multiple vulnerabilities that exists in their IBM Q radar use case manager app and IBM DB2 products which leads attackers to perform malicious activities. IBM highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM QRadar Use Case Manager v1.0 – v3.4.0 IBM Db2 9.7.x, 10.1.x, 10.5.x, 11.1.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-use-case-manager-app-is-vulnerable-to-using-components-with-known-vulnerabilities/ https://www.ibm.com/blogs/psirt/security-bulletin-ibm-db2-is-affected-by-multiple-vulnerabilities-in-the-included-expat-3rd-party-library-cve-2022-23852-and-cve-2022-23990/

Affected Product	Drupal
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities
Description	Drupal has released security updates addressing vulnerabilities including improper input validation which could allow an attacker to inject disallowed values or overwrite data and access bypass for users who have access to use revisions of content generally. Drupal highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Drupal 9.3 Drupal 9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2022-008 https://www.drupal.org/sa-core-2022-009

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20732, CVE-2022-20773, CVE-2022-20783, CVE-2022-20778, CVE-2022-20795, CVE-2022-20805, CVE-2022-20790, CVE-2022-20804, CVE-2022-20787, CVE-2022-20786, CVE-2022-20788, CVE-2022-20789)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the most severe vulnerabilities could cause information disclosure, virtual appliance impersonation, denial of service, cross-site scripting, bypass the SSL decryption, arbitrary file read/write, cross-site request forgery, SQL injection. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco VIM Cisco Umbrella Virtual Appliance for both VMWare ESXi and Hyper-V running a software version earlier than 3.3.2 Cisco RoomOS Software Cisco Webex Meetings ASA Software Release 9.16.3 or earlier ASA Software Release 9.17.1.9 or earlier FTD Software Release 7.0.1 or earlier FTD Software Release 7.1.0.1 or earlier Cisco Unified CM and Unified CM SME Cisco Unified CM IM&P Unity Connection
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vim-privesc-T2tsFUf https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uva-static-key-6RQTRs4c https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ce-roomos-dos-c65x2Qf2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-w47AMqAk https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vpndtls-dos-TunzLEV https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uswg-fdbps-xtTRKpp6 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-file-read-h8h4HEJ3 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-dos-zHS9X9kD https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-csrf-jrKP4eNT https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-sqlinj-GrpUuQEJ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-6MCe4kPF https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-arb-write-74QzruUU

Affected Product	Dell
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2019-14584, CVE-2021-28210, CVE-2021-28211)
Description	Dell has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the most severe vulnerabilities could cause authentication bypass and buffer overflow. Dell highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Dell PowerEdge Server BIOS - Tianocore EDK2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000198065/dsa-2022-088

Affected Product	Redhat
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-21426, CVE-2022-21434, CVE-2022-21443, CVE-2022-21476, CVE-2022-21496, CVE-2022-21449)
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the most severe vulnerabilities could cause information disclosure, denial of service, unauthorized update, insert or delete data. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Red Hat Satellite 6.9 x86_64 Red Hat Satellite Capsule 6.9 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:1478 https://access.redhat.com/errata/RHSA-2022:1442 https://access.redhat.com/errata/RHSA-2022:1444 https://access.redhat.com/errata/RHSA-2022:1445 https://access.redhat.com/errata/RHSA-2022:1440 https://access.redhat.com/errata/RHSA-2022:1443 https://access.redhat.com/errata/RHSA-2022:1441

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.