Advisory Alert

Alert Number: AAA20230112 **Date:** January 12, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Juniper	**High**, Medium	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Drupal	**Medium**	Access Bypass Vulnerability

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2022-29154, CVE-2022-2526, CVE-2022-21541, CVE-2022-34169, CVE-2022-21540, CVE-2022-21624, CVE-2022-21626, CVE-2022-21628, CVE-2022-21619, CVE-2007-2285, CVE-2018-8046, CVE-2020-26137, CVE-2021-3177, CVE-2020-26116, CVE-2022-1729, CVE-2022-32250, CVE-2022-1271, CVE-2021-3156, CVE-2020-14145, CVE-2020-14871, CVE-2020-15778, CVE-2020-1971, CVE-2020-28196, CVE-2021-2144, CVE-2021-2146, CVE-2021-2154, CVE-2021-2160, CVE-2021-2162, CVE-2021-2166, CVE-2021-2169, CVE-2021-2171, CVE-2021-2174, CVE-2021-2178, CVE-2021-2179, CVE-2021-2180, CVE-2021-2194, CVE-2021-2202, CVE-2021-2226, CVE-2021-2307, CVE-2021-23841, CVE-2021-2342, CVE-2021-2372, CVE-2021-2385, CVE-2021-2389, CVE-2021-2390, CVE-2021-3450, CVE-2021-23017, CVE-2021-35940, CVE-2022-0934)
Description	Juniper has released a security update for multiple critical vulnerabilities that exist in Juniper Junos Space and Juniper Contrail Service Orchestration. Successful exploitation of the most severe vulnerabilities can lead to heap-based buffer overflow, privilege escalation, use-after-free vulnerability and arbitrary file execution. Juniper highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Juniper Networks Junos Space versions prior to 22.3R1 Juniper Networks Contrail Service Orchestration (CSO) prior to 6.3.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-22-3R1-release https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Contrail-Service-Orchestration-Multiple-vulnerabilities-resolved-in-CSO-6-3-0

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20025, CVE-2023-20026)
Description	Cisco has released a security update addressing multiple vulnerabilities that exist in Cisco Small Business RV016, RV042, RV042G, and RV082 Routers. If exploited these vulnerabilities could cause authentication bypass or arbitrary command execution on the underlying operating system of an affected device. Cisco highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	RV016 Multi-WAN VPN Routers RV042 Dual WAN VPN Routers RV042G Dual Gigabit WAN VPN Routers RV082 Dual WAN VPN Routers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-45047, CVE-2021-30483)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities can lead to unsafe deserialization or Directory traversal. **CVE-2022-45047-** A vulnerability was found in Apache MINA SSHD, when using Java deserialization to load a serialized java.security.PrivateKey. An attacker could benefit from unsafe deserialization by inserting unsecured data that may affect the application or server. **CVE-2021-30483-** A vulnerability was found in isomorphic-git. An attacker could cause a Directory Traversal via a crafted file path in a repository being cloned. Redhat recommends to apply necessary fixes to avoid issues.
Affected Products	Red Hat Virtualization Manager 4.4 x86_64 Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Virtualization for IBM Power LE 4 for RHEL 8 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:0074

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (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)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities can lead to arbitrary code execution, denial of service and information disclosure. Dell recommends to apply the necessary security updates at your earliest to avoid issue.
Affected Products	Dell PowerEdge R6415 Before 1.18.0 Dell PowerEdge R7415 Before 1.18.0 Dell PowerEdge R7425 Before 1.18.0 Dell PowerEdge C6525 Before 2.9.3 Dell PowerEdge R7425 Before 2.9.4 Dell PowerEdge R6515 Before 2.9.3 Dell PowerEdge R7515 Before 2.9.3 Dell PowerEdge R6525 Before 2.9.3 Dell PowerEdge R7525 Before 2.9.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000207371/dsa-2023-002-dell-poweredge-server-security-update-for-amd-server-vulnerabilities

Affected Product	**Juniper**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-22410, CVE-2022-0778, CVE-2022-1473, CVE-2023-22404, CVE-2023-22417, CVE-2023-22413, CVE-2023-22411, CVE-2023-22396, CVE-2023-22393, CVE-2023-22394, CVE-2023-22391, CVE-2023-22412, CVE-2023-22415, CVE-2023-22401, CVE-2023-22416, CVE-2023-22399, CVE-2019-11287, CVE-2023-22408, CVE-2023-22403, CVE-2023-22400, CVE-2023-22395, CVE-2023-22402, CVE-2023-22414, CVE-2023-22398, CVE-2023-22406, CVE-2023-22409, CVE-2023-22407, CVE-2023-22405, CVE-2023-22397)
Description	Juniper has released a security update addressing multiple vulnerability that exists in their products. If exploited these vulnerabilities could cause denial of service and memory leakage Juniper highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Multiple products and versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=%40sfcec_community_publish_date_formula__c%20---descending-&f:ctype=[Security%20Advisories]&f:slevel=[High] https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=relevancy&f:ctype=[Security%20-Advisories]&f:slevel=[Medium]

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20019, CVE-2023-20058, CVE-2023-20043, CVE-2023-20044, CVE-2023-20047, CVE-2023-20040, CVE-2023-20002, CVE-2023-20008, CVE-2023-20045, CVE-2023-20007, CVE-2023-20020, CVE-2023-20037, CVE-2023-20038, CVE-2023-20018)
Description	Cisco has released security updates addressing multiple vulnerabilities in their products. Most severe vulnerabilities could cause authentication bypass, remote code execution, denial of service and memory leakage Cisco recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Cisco BroadWorks Application Delivery Platform 22.0 and earlier, 23.0, 24.0 Cisco BroadWorks Application Delivery Platform Device Management Release 22.0 Cisco BroadWorks Application Server 22.0 and earlier, 23.0, 24.0 Cisco BroadWorks Xtended Services Platform 22.0 and earlier, 23.0 Cisco IND Release 1 Cisco NSO Release 3.3 through 5.3 5.4, 5.5, 5.6, 5.7, 5.8 Cisco Packaged CCE Release 12.0(1)1 and earlier, 12.5(1), 12.5(1) SU2 Cisco RV340 and RV345 Series Routers Release earlier than 1.0.03.29 Cisco SIP Software Releas earlier than 14.1(1)SR2 in IP Phone 7800 and 8800 Series (Except Wireless IP Phone 8821) Cisco SIP Software Release earlier than 11.0(6)SR4 in Wireless IP Phone 8821 Cisco TelePresence CE Software Release 9, 10 Cisco Unified CCE Release 12.0(1)1 and earlier, 12.5(1), 12.5(2), 12.6(1) Cisco Unified CCX Release 12.0(1)1 and earlier, 12.5(1), 12.5(1) SU2 Cisco Unified Intelligence Center Release 12.0(1)1 and earlier, 12.5(1), 12.6(1), 12.6(1) ES2 Cisco Webex Room Phone and Cisco Webex Share Firmware Release 1.2.0 and earlier RV160 VPN Routers RV160W Wireless-AC VPN Routers RV260 VPN Routers RV260P VPN Routers with PoE RV260W Wireless-AC VPN Routers RV340 Dual WAN Gigabit VPN Routers RV340W Dual WAN Gigabit Wireless-AC VPN Routers RV345 Dual WAN Gigabit VPN Routers RV345P Dual WAN Gigabit POE VPN Routers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-xss-EzqDXqG4 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuis-xss-Omm8jyBX https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cxagent-gOq9QjqZ https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lldp-memlk-McOecPT https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-zjBeMkZg https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-cmd-exe-n47kJQLE https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-dos-HpkeYzp https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ind-fZyVjJtG https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Access Bypass Vulnerability
Description	Drupal has released a security update to address an access bypass vulnerability that exist in Private Taxonomy terms module of Drupal. Using this vulnerability, an attacker with permission to "Administer own taxonomy" or "View private taxonomies" roles can create ‘private’ vocabularies. Drupal recommends to apply the necessary security updates at your earliest to avoid issue.
Affected Products	Private Taxonomy Terms module versions prior to 8.x-2.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2023-001

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.