Advisory Alert

Alert Number: AAA20230622 **Date:** June 22, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
RedHat	**High**	Multiple Vulnerabilities
Juniper	**High**	Improper Input Validation Vulnerability
Ubuntu	**High, Medium**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2022-32532, CVE-2022-40664, CVE-2021-20294, CVE-2021-20284, CVE-2021-20197, CVE-2020-16590, CVE-2020-16591, CVE-2020-16592, CVE-2020-16593, CVE-2020-16599, CVE-2021-3487, CVE-2020-35448, CVE-2020-35493, CVE-2020-35496, CVE-2020-35507, CVE-2022-23491, CVE-2022-28735, CVE-2022-28736, CVE-2022-28737, CVE-2022-21541, CVE-2022-34169, CVE-2022-21540, CVE-2022-21476, CVE-2022-21443, CVE-2022-21434, CVE-2022-21496, CVE-2022-21426, CVE-2021-35603, CVE-2021-35586, CVE-2021-35567, CVE-2021-35565, CVE-2021-35564, CVE-2021-35561, CVE-2021-35556, CVE-2021-35550, CVE-2021-35559, CVE-2021-35578, CVE-2021-2388, CVE-2021-2369, CVE-2021-2341, CVE-2021-46848, CVE-2022-2097, CVE-2022-1292, CVE-2022-2068, CVE-2021-46827, CVE-2022-45061, CVE-2018-8088, CVE-2021-45079, CVE-2021-41991, CVE-2021-41990, CVE-2019-13990, CVE-2022-24801, CVE-2022-21712, CVE-2023-32449)
Description	Dell has released a security update addressing Multiple Vulnerabilities that exists in their products. If exploited theses vulnerabilities could lead to Authentication Bypass, arbitrary code execution, Integer Overflow. Dell highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PowerStore 500T PowerStoreT OS Versions prior to 3.5.0.0-2050321 PowerStore 1000T PowerStoreT OSVersions prior to 3.5.0.0-2050321 PowerStore 1200T PowerStoreT OSVersions prior to 3.5.0.0-2050321 PowerStore 3000T PowerStoreT OSVersions prior to 3.5.0.0-2050321 PowerStore 3200T PowerStoreT OSVersions prior to 3.5.0.0-2050321 PowerStore 5000T PowerStoreT OSVersions prior to 3.5.0.0-2050321 PowerStore 5200T PowerStoreT OSVersions prior to 3.5.0.0-2050321 PowerStore 7000T PowerStoreT OSVersions prior to 3.5.0.0-2050321 PowerStore 9000T PowerStoreT OSVersions prior to 3.5.0.0-2050321 PowerStore 9200T PowerStoreT OSVersions prior to 3.5.0.0-2050321
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000215171/dsa-2023-173-dell-powerstore-family-security-update-for-multiple-vulnerabilities

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20860, CVE-2023-20861, CVE-2023-2235, CVE-2023-32233)
Description	RedHat has released security updates addressing Multiple Vulnerabilities exists in their products. If exploited theses vulnerabilities could lead to use-after-free condition, denial of service and security bypass. RedHat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization for IBM Power LE 4 for RHEL 8 ppc64le Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Virtualization Manager 4.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:3705 https://access.redhat.com/errata/RHSA-2023:3771

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Improper Input Validation Vulnerability (CVE-2023-0026)
Description	Juniper has released a security update addressing an Improper Input Validation Vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved. By sending a compromised BGP update message that contains a specific optional transitive attribute, an unauthenticated network-based attacker can terminate a BGP session. Since the respective attribute can propagate through unaffected systems, continuous receipt of a BGP update containing this attribute will create a sustained Denial of Service (DoS) condition. Juniper recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Juniper Networks Junos OS: • 15.1R1 and later versions prior to 20.4R3-S8; • 21.1 version 21.1R1 and later versions prior to 21.2R3-S6; • 21.3 versions prior to 21.3R3-S5; • 21.4 versions prior to 21.4R3-S4; • 22.1 versions prior to 22.1R3-S4; • 22.2 versions prior to 22.2R3-S2; • 22.3 versions prior to 22.2R3-S2; • 22.4 versions prior to 22.4R2-S1, 22.4R3; • 23.1 versions prior to 23.1R1-S1, 23.1R2. Juniper Networks Junos OS Evolved: • All versions prior to 20.4R3-S8-EVO; • 21.1 version 21.1R1-EVO and later versions prior to 21.2R3-S6-EVO; • 21.3 versions prior to 21.3R3-S5-EVO; • 21.4 versions prior to 21.4R3-S4-EVO; • 22.1 versions prior to 22.1R3-S4-EVO; • 22.2 versions prior to 22.2R3-S2-EVO; • 22.3 versions prior to 22.3R2-S2-EVO, 22.3R3-S1-EVO; • 22.4 versions prior to 22.4R2-S1-EVO, 22.4R3-EVO; • 23.1 versions prior to 23.1R1-S1-EVO, 23.1R2-EVO.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2023-06-Out-of-Cycle-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-BGP-session-will-flap-upon-receipt-of-a-specific-optional-transitive-attribute-CVE-2023-0026?language=en_US

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-32233, CVE-2023-2612, CVE-2023-0386, CVE-2023-1872, CVE-2023-1380, CVE-2023-31436)
Description	Ubuntu has released a security update addressing Multiple Vulnerabilities in their products. If exploited theses vulnerabilities could lead to denial of service, sensitive information disclosure and arbitrary code execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 22.04 LTS Ubuntu 20.04 LTS Ubuntu 18.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/LSN-0095-1

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20028, CVE-2023-20119, CVE-2023-20120, CVE-2023-20199)
Description	Cisco has released security updates addressing Multiple Vulnerabilities in their products. If exploited theses vulnerabilities could lead to Authentication Bypass and Cross-Site Scripting. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco Duo Two-Factor Authentication for macOS Release 2.0.0 Secure Email and Web Manager with Cisco AsyncOS Release 15.0 Secure Email Gateway with Cisco AsyncOS Release 15.0 Secure Web Appliance with Cisco AsyncOS Release 15.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-mac-bypass-OyZpVPnx https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-wsa-xss-cP9DuEmq

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.