Advisory Alert

Alert Number: AAA20240208 **Date:** February 8, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Cross-Site Request Forgery Vulnerabilities
Juniper	**Critical**	Multiple Vulnerabilities
Redhat	**High**	Kernel Security Updates
cPanel	**High**	Security Updates
SonicWall	**High**	Improper Authentication Vulnerability
Cisco	**High**	Denial of Service Vulnerability
Ubuntu	**High**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Cross-Site Request Forgery Vulnerabilities (CVE-2024-20252 , CVE-2024-20254, CVE-2024-20255)
Description	Cisco has released security updates addressing Cross-Site Request Forgery Vulnerabilities that exist Cisco Expressway Series. These vulnerabilities could allow an unauthenticated, remote attacker to conduct cross-site request forgery (CSRF) attacks, which could allow the attacker to perform arbitrary actions on an affected device. Cisco recommends to apply the necessary software updates to avoid issue
Affected Products	Cisco Expressway Series Release Earlier than 14.0 Cisco Expressway Series 14.0 Cisco Expressway Series 15.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-csrf-KnnZDMj3

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35116, CVE-2023-34453, CVE-2023-34455, CVE-2023-34454, CVE-2023-43642, CVE-2023-2976, CVE-2023-33201,CVE-2023-46136,CVE-2023-43804,CVE-2023-37920, CVE-2022-25883, CVE-2023-45133, CVE-2023-31484, CVE-2023-1370, CVE-2021-4048, CVE-2021-23445, CVE-2021-31684, CVE-2023-38019, CVE-2023-38020, CVE-2023-38263, CVE-2023-46308, CVE-2023-32006, CVE-2023-32002, CVE-2023-32559, CVE-2022-38900, CVE-2023-45857, CVE-2022-25927)
Description	Juniper has released a security update addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to denial of service, integer overflow, LDAP injection, Improper Input Validation. Juniper recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Log Collector Application prior to version v1.8.4 SOAR Plugin Application prior to version 5.3.1 Deployment Intelligence Application prior to 3.0.12 User Behavior Analytics Application add-on prior to 4.1.14 Pulse Application add-on prior to 2.2.12 Assistant Application add-on prior to 3.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved-in-JSA-Applications?language=en_US

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Kernel security updates (CVE-2021-3640, CVE-2021-4204, CVE-2021-30002, CVE-2021-34866, CVE-2022-0168, CVE-2022-0500, CVE-2022-0617, CVE-2022-1462, CVE-2022-2078, CVE-2022-2586, CVE-2022-2663, CVE-2022-3524, CVE-2022-3545, CVE-2022-3566, CVE-2022-3594, CVE-2022-3619, CVE-2022-3623, CVE-2022-3707, CVE-2022-21499, CVE-2022-23222, CVE-2022-24448, CVE-2022-25265, CVE-2022-28388, CVE-2022-28390, CVE-2022-28893, CVE-2022-36946, CVE-2022-39189, CVE-2022-45887, CVE-2023-0458, CVE-2023-1075, CVE-2023-1252, CVE-2023-1989, CVE-2023-2166, CVE-2023-2176, CVE-2023-3141, CVE-2023-4132, CVE-2023-4921, CVE-2023-5717, CVE-2023-6356, CVE-2023-6535, CVE-2023-6536, CVE-2023-6610, CVE-2023-6817, CVE-2023-6932, CVE-2023-20569, CVE-2023-23455, CVE-2023-28328, CVE-2023-28772, CVE-2023-35825,CVE-2023-40283,CVE-2023-45862,CVE-2023-46813, CVE-2024-0646, CVE-2023-1074, CVE-2023-6356, CVE-2023-6535, CVE-2023-6536, CVE-2023-6606, CVE-2023-6610, CVE-2023-6932, CVE-2023-7192, CVE-2023-45862, CVE-2024-0646)
Description	Redhat has released a security update addressing Linux Kernel Security updates affecting their products. Exploitation of these vulnerabilities could lead multiple security flows. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0725 https://access.redhat.com/errata/RHSA-2024:0724

Affected Product	**cPanel**
Severity	**High**
Affected Vulnerability	Security Updates (CVE-2024-0853)
Description	cPanel has released updates addressing security fixes that exist in EasyApache 4 with libcurl. It is strongly encouraged that all libcurl users upgrade to the latest version.
Affected Products	All versions of libcurl through 8.5.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2024-02-07-maintenance-and-security-release/

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Improper Authentication Vulnerability (CVE-2024-22394)
Description	SonicWall has released security updates addressing improper authentication vulnerability that exist in the SonicOS. The vulnerability has been identified in SonicWall SonicOS SSL-VPN feature, which in specific conditions could allow a remote attacker to bypass authentication. This issue affects only firmware version SonicOS 7.1.1-7040. SonicWall recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SonicOS 7.1.1-7040 Gen7 - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSv 270, NSv 470, NSv 870
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0003

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-20290)
Description	Cisco has released security updates addressing Denial of Service Vulnerability that exist Secure Endpoint Connector for Windows. This vulnerability is due to an incorrect check for end-of-string values during scanning, which may result in a heap buffer over-read. An attacker could exploit this vulnerability by submitting a crafted file containing OLE2 content to be scanned by ClamAV on an affected device Cisco recommends to apply the necessary software updates to avoid issue
Affected Products	Secure Endpoint Connector for Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-hDffu6t

Affected Product	**Ubuntu**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5345, CVE-2023-6040, CVE-2023-6176, CVE-2023-6817, CVE-2023-6932, CVE-2023-34324, CVE-2023-35827, CVE-2023-46813, CVE-2023-46862, CVE-2023-5972, CVE-2023-6176, CVE-2023-6531, CVE-2023-6622, CVE-2024-0641, CVE-2023-45863, CVE-2023-46343, CVE-2023-32250, CVE-2023-32252, CVE-2023-32257)
Description	Ubuntu has released security updates addressing multiple vulnerabilities within 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 18.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 23.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/LSN-0100-1 https://ubuntu.com/security/notices/USN-6624-1 https://ubuntu.com/security/notices/USN-6625-1 https://ubuntu.com/security/notices/USN-6626-1

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.