Advisory Alert

Alert Number: AAA20240913 **Date:** September 13, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
NetApp	**Critical**	Security Update
Juniper	**High**	Improper Input Validation vulnerability
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**Medium**	Multiple Vulnerabilities
F5	**Medium**	Security Update

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38475, CVE-2024-38473, CVE-2024-39573, CVE-2024-38477, CVE-2024-38476, CVE-2024-38474, CVE-2023-38709)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These security vulnerabilities could be exploited by malicious users to compromise the affected system Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	CyberSense OS Update Versions prior to 1.5.0-47
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000228534/dsa-2024-374-security-update-for-dell-cyber-sense-for-third-party-vulnerabilities

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2023-37920)
Description	NetApp has issued a security update addressing a vulnerability that exists in 'Certif' third-party product. If the vulnerability is exploited, it could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Certifi versions 2015.04.28 prior to 2023.07.22 in; • Management Services for Element Software and NetApp HCI • ONTAP Mediator
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240912-0002/

Affected Product	**Juniper**	
Severity	**High**	
Affected Vulnerability	Improper Input Validation Vulnerability (CVE-2023-4481)	
Description	Juniper has released security updates addressing an Improper Input Validation vulnerability that exists in their products. If exploited this vulnerability could allow an unauthenticated, network-based attacker to cause a Denial of Service (DoS). Juniper advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	Junos OS: • All versions before 20.4R3-S10 • from 21.1 through 21.1R1* • from 21.2 before 21.2R3-S5 • from 21.3 before 21.3R3-S5 • from 21.4 before 21.4R3-S5 • from 21.4R3-S6 before 21.4R3-S7 • from 22.1 before 22.1R3-S4 • from 22.2 before 22.2R3-S3 • from 22.3 before 22.3R3-S1 • from 22.4 before 22.4R3 • from 23.2 before 23.2R2	Junos OS Evolved: • All versions before 20.4R3-S10-EVO • from 21.2-EVO before 21.2R3-S7-EVO • from 21.3-EVO before 21.3R3-S5-EVO • from 21.4-EVO before 21.4R3-S5-EVO • from 22.1-EVO before 22.1R3-S4-EVO • from 22.2-EVO before 22.2R3-S3-EVO • from 22.3-EVO before 22.3R3-S1-EVO • from 22.4-EVO before 22.4R3-EVO • from 23.2-EVO before 23.2R2-EVO
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://supportportal.juniper.net/s/article/2023-08-29-Out-of-Cycle-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-crafted-BGP-UPDATE-message-allows-a-remote-attacker-to-de-peer-reset-BGP-sessions-CVE-2023-4481?language=en_US	

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause memory leakage, use-after-free conditions, race conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.2, 5.3, 5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243225-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243227-1/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7003-2

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-23984, CVE-2024-24968)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products **CVE-2024-23984** - A security vulnerability in HPE ProLiant DL/XL, Synergy, and Edgeline servers using certain Intel processors could be locally exploited to allow disclosure of information. **CVE-2024-24968** - A security vulnerability in HPE ProLiant DL/XL, Synergy, and Edgeline servers using certain Intel processors could be locally exploited to allow denial of service. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.20_08-07-2024 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.20_08-07-2024 HPE Compute Edge Server e930t - Prior to v2.32_09-09-2024 HPE Edgeline e920 Server Blade - Prior to v2.20_08-07-2024 HPE Edgeline e920d Server Blade - Prior to v2.20_08-07-2024 HPE Edgeline e920t Server Blade - Prior to v2.20_08-07-2024 HPE Apollo 2000 Gen10 Plus System - Prior to v2.20_08-07-2024 HPE Apollo 4200 Gen10 Plus System - Prior to v2.20_08-07-2024 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.20_08-07-2024 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.20_08-07-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04702en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04701en_us&docLocale=en_US

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Security Update (**CVE-2024-25629**)
Description	F5 has released a security update addressing a vulnerability that exists in the F5 Traffix SDC. **CVE-2024-25629** - c-ares is a C library for asynchronous DNS requests. `ares__read_line()` is used to parse local configuration files such as `/etc/resolv.conf`, `/etc/nsswitch.conf`, the `HOSTALIASES` file, and if using a c-ares version prior to 1.27.0, the `/etc/hosts` file. If any of these configuration files has an embedded `NULL` character as the first character in a new line, it can lead to attempting to read memory prior to the start of the given buffer which may result in a crash. This issue is fixed in c-ares 1.27.0. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5 Traffix SDC 5.1.0 - 5.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000141051

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.