Advisory Alert

Alert Number: AAA20250220 **Date:** February 20, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Arbitrary Code Execution Vulnerability
Drupal	**Critical**	Cross Site Scripting Vulnerability
Red Hat	**High**	Arbitrary Code Execution Vulnerability
F5	**High**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Linux kernel Vulnerability
Drupal	**Medium**	Multiple Vulnerabilities
CPanel	**Medium**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability
Description	HPE has released security updates addressing a cross site scripting vulnerability that exist in their products. **CVE-2021-44228 -** Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Telco Service Orchestrator - 3.7.1 - Closed Loop snmp adapter
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04217en_us&docLocale=en_US

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability
Description	Drupal has released security updates addressing an arbitrary code execution vulnerability that exist in their products. Exploitation of these vulnerabilities may lead to compromise the effected system. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal 10.3.x, Prior to Drupal 10.3.13 Drupal 10.4.x, Prior to Drupal 10.4.3 Drupal 11.0.x, Prior to Drupal 11.0.12 Drupal 11.1.x, Prior to Drupal 11.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2025-001

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2024-53104)
Description	Red Hat has released security updates addressing an arbitrary code execution vulnerability that exists in their products. **CVE-2024-53104 -** A vulnerability was found in the Linux kernel's USB Video Class driver. A buffer for video frame data is allocated, which does not account for all of the frame formats contained in a video stream, leading to an out-of-bounds write when a stream includes frames with an undefined format. An attacker who is able to influence the format of video streams captured by a system's USB video device could exploit this flaw to alter system memory and potentially escalate their privileges or execute arbitrary code. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:1680

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	F5 has released security updates addressing Multiple Vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Information Disclosure, Data Leakage and Denial-of-service. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Traffix SDC Versions - 5.2.0 Traffix SDC Versions - 5.2.0 BIG-IP Next (LTM) Versions - 20.2.0 - 20.3.0 BIG-IP Next SPK Versions - 1.7.0 - 1.9.2 BIG-IP Next CNF Versions - 1.1.0 - 1.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000149858 • https://my.f5.com/manage/s/article/K000149857 • https://my.f5.com/manage/s/article/K000149304

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Privilege escalation Vulnerabilities (CVE-2024-6387, CVE-2024-38796)
Description	Dell has released security updates addressing Multiple Vulnerabilities that exist in their products. If 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	S5448F-ON Firmware Versions prior to 3.52.5.1-12 Z9432F-ON Firmware Versions prior to 3.51.5.1-21 Z9664F-ON Firmware Versions prior to 3.54.5.1-9 PowerEdge R650 BIOS Versions prior to 1.16.2 PowerEdge R750 BIOS Versions prior to 1.16.2 PowerEdge R750XA BIOS Versions prior to 1.16.2 PowerEdge C6520 BIOS Versions prior to 1.16.2 PowerEdge MX750C BIOS Versions prior to 1.16.2 PowerEdge R550 BIOS Versions prior to 1.16.2 PowerEdge R450 BIOS Versions prior to 1.16.2 PowerEdge R650XS BIOS Versions prior to 1.16.2 PowerEdge R750XS BIOS Versions prior to 1.16.2 PowerEdge T550 BIOS Versions prior to 1.16.2 PowerEdge XR11 BIOS Versions prior to 1.16.2 PowerEdge XR12 BIOS Versions prior to 1.16.2 PowerEdge XR4510c BIOS Versions prior to 1.17.3 PowerEdge XR4520c BIOS Versions prior to 1.17.3 PowerEdge T150 BIOS Versions prior to 1.11.1 PowerEdge T350 BIOS Versions prior to 1.11.1 PowerEdge R250 BIOS Versions prior to 1.11.1 PowerEdge R350 BIOS Versions prior to 1.11.1 PowerEdge R740 BIOS Versions prior to 2.23.0 PowerEdge R740XD BIOS Versions prior to 2.23.0 PowerEdge R640 BIOS Versions prior to 2.23.0 PowerEdge R940 BIOS Versions prior to 2.23.0 PowerEdge R540 BIOS Versions prior to 2.23.0 PowerEdge R440 BIOS Versions prior to 2.23.0 PowerEdge T440 BIOS Versions prior to 2.23.0 PowerEdge XR2 BIOS Versions prior to 2.23.0 PowerEdge R740XD2 BIOS Versions prior to 2.23.0 PowerEdge R840 BIOS Versions prior to 2.23.0 PowerEdge R940XA BIOS Versions prior to 2.23.0 PowerEdge T640 BIOS Versions prior to 2.23.0 PowerEdge C6420 BIOS Versions prior to 2.23.0 PowerEdge FC640 BIOS Versions prior to 2.23.0 PowerEdge M640BIOS Versions prior to 2.23.0 PowerEdge M640 (for PE VRTX) BIOS Versions prior to 2.23.0 PowerEdge MX740C BIOS Versions prior to 2.23.0 PowerEdge MX840C BIOS Versions prior to 2.23.0 PowerEdge C4140 BIOS Versions prior to 2.23.0 PowerEdge T140 BIOS Versions prior to 2.18.0 PowerEdge T340 BIOS Versions prior to 2.18.0 PowerEdge R240 BIOS Versions prior to 2.18.0 PowerEdge R340 BIOS Versions prior to 2.18.0 Dell EMC Storage NX3240 BIOS Versions prior to 2.23.0 Dell EMC Storage NX3340 BIOS Versions prior to 2.23.0 Dell EMC NX440 BIOS Versions prior to 2.18.0 Dell EMC XC Core XC450 BIOS Versions prior to 1.16.2 Dell EMC XC Core XC650 BIOS Versions prior to 1.16.2 Dell EMC XC Core XC750 BIOS Versions prior to 1.16.2 Dell EMC XC Core XC750xaBIOS Versions prior to 1.16.2 Dell EMC XC Core XC6520 BIOS Versions prior to 1.16.2 Dell EMC XC Core 6420 System BIOS Versions prior to 2.23.0 Dell EMC XC Core XC640 System BIOS Versions prior to 2.23.0 Dell EMC XC Core XC740xd System BIOS Versions prior to 2.23.0 Dell EMC XC Core XC740xd2 BIOS Versions prior to 2.23.0 Dell EMC XC Core XC940 System BIOS Versions prior to 2.23.0 Dell EMC XC Core XCXR2 BIOS Versions prior to 2.23.0 PowerEdge R6615 BIOS Versions prior to 1.11.2 PowerEdge R7615 BIOS Versions prior to 1.11.2 PowerEdge R6625 BIOS Versions prior to 1.11.2 PowerEdge R7625 BIOS Versions prior to 1.11.2 PowerEdge C6615 BIOS Versions prior to 1.6.2 PowerEdge R6515 BIOS Versions prior to 2.18.1 PowerEdge R6525 BIOS Versions prior to 2.18.1 PowerEdge R7515 BIOS Versions prior to 2.18.1 PowerEdge R7525 BIOS Versions prior to 2.18.1 PowerEdge C6525 BIOS Versions prior to 2.18.1 PowerEdge XE8545 BIOS Versions prior to 2.17.1 Dell EMC XC Core XC7525 BIOS Versions prior to 2.18.1 Dell XC Core XC7625BIOSVersions prior to 1.11.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000287177/dsa-2025-099-security-update-for-dell-networking-z9432f-on-z9664f-on-and-s5448f-on-vulnerability • https://www.dell.com/support/kbdoc/en-us/000287202/dsa-2025-038-security-update-for-dell-poweredge-server-bios-for-tianocore-edk2-vulnerability

Affected Product	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-45046, CVE-2024-38827, CVE-2024-56337, CVE-2024-50379, CVE-2024-21538))
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service (DoS), Unauthorized Arbitrary File Creation, Unauthorized Remote Access, Arbitrary Code Execution. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Telco Service Orchestrator - 3.7.1 - Closed Loop snmp adapter HPE Telco Service Orchestrator - Prior to v4.2.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04217en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04806en_us&docLocale=en_US

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Linux kernel Vulnerability
Description	HPE has released security updates addressing a Linux kernel Vulnerability that exists in their products. An attacker could use a specially crafted file system image that, when mounted, could cause a denial of service (system crash) or possibly execute arbitrary code. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7276-1

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing Multiple Vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Access bypass and Gadget Chain. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal 10.3.x, Prior to Drupal 10.3.13 Drupal 10.4.x, Prior to Drupal 10.4.3 Drupal 11.0.x, Prior to Drupal 11.0.12 Drupal 11.1.x, Prior to Drupal 11.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-core-2025-002 • https://www.drupal.org/sa-core-2025-003

Affected Product	**CPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-24928, CVE-2024-56171)
Description	CPanel has released security updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2025-24928 -** libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a stack-based buffer overflow in xmlSnprintfElements in valid.c. To exploit this, DTD validation must occur for an untrusted document or untrusted DTD. **CVE-2024-56171 -** libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a use-after-free in xmlSchemaIDCFillNodeTables and xmlSchemaBubbleIDCNodeTables in xmlschemas.c. To exploit this, a crafted XML document must be validated against an XML schema with certain identity constraints, or a crafted XML schema must be used. CPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of libxml2 through 2.13.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-6-maintenance-and-security-release/

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20211, CVE-2025-20153, CVE-2025-20158)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2025-20211 -** A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform could allow an unauthenticated, remote attacker to conduct a cross-site scripting attack against a user of the interface. **CVE-2025-20153 -** A vulnerability in the email filtering mechanism of Cisco Secure Email Gateway could allow an unauthenticated, remote attacker to bypass the configured rules and allow emails that should have been denied to flow through an affected device. **CVE-2025-20158 -** A vulnerability in the debug shell of Cisco Video Phone 8875 and Cisco Desk Phone 9800 Series could allow an authenticated, local attacker to access sensitive information on an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials with SSH access on the affected device. SSH access is disabled by default. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco BroadWorks Call Center application - 24.0, 26.0 Cisco BroadWorks Receptionist application was installed - 24.0, 26.0 Cisco AsyncOS Software for Secure Email Gateway Release - 14.2 and Prior Cisco SIP Software Release - 3.2(1) and Prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-GDPgJ58P • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-mailpol-bypass-5nVcJZMw • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-info-disc-YyxsWStK

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.