Advisory Alert

Alert Number: AAA20250402 **Date:** April 2, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
IBM	**High**	Denial of Service Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Kernel Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These 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	Dell Unity Dell Unity Operating Environment (OE) - Versions prior to 5.5.0.0.5.259 Dell UnityVSA Dell Unity Operating Environment (OE) - Versions prior to 5.5.0.0.5.259 Dell Unity XT Dell Unity Operating Environment (OE) - Versions prior to 5.5.0.0.5.259
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20439, CVE-2024-20440)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-20439 -** A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to log in to an affected system by using a static administrative credential. **CVE-2024-20440 -** A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to access sensitive information. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Smart Licensing Utility Release - 2.0.0, 2.1.0, 2.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2025-23184)
Description	IBM has released security updates addressing a Denial of Service Vulnerability that exists in their products. **CVE-2025-23184 -** There is a vulnerability in the Apache CXF library used by IBM WebSphere Application Server Liberty, which is bundled with IBM WebSphere Hybrid Edition, with the jaxws-2.2, xmlWS-3.0 or xmlWS-4.0 feature enabled. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Hybrid Edition - Version 5.1 IBM WebSphere Application Server Liberty - Version 17.0.0.3 - 25.0.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7229768

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47535, CVE-2025-23367, CVE-2025-24970, CVE-2025-25193)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, System crash, Privilege Escalation. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:3467

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3661, CVE-2025-25041)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-3661 -** A vulnerability in the network configuration service of the DHCP protocol could allow an unauthenticated remote attacker to intercept VPN traffic. Successful exploitation could allow an attacker to read, disrupt, or possibly modify network traffic that was expected to be protected by the VPN. **CVE-2025-25041 -** A vulnerability in the HPE Aruba Networking Virtual Intranet Access (VIA) client could allow malicious users to overwrite arbitrary files as NT AUTHORITY\SYSTEM (root). A successful exploit could allow the creation of a Denial-of-Service (DoS) condition affecting the Microsoft Windows Operating System. This vulnerability does not affect Linux and Android based clients. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking VIA client : 4.7.0 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04841en_us&docLocale=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Kernel Vulnerabilities (CVE-2022-48791, CVE-2024-41062)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise High Performance Computing 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20251088-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251092-1/

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.