Advisory Alert

Alert Number: AAA20250327 **Date:** March 27, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Out-of-bounds Write Vulnerability
Cisco	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29133, CVE-2024-29131, CVE-2023-33202, CVE-2024-34447, CVE-2024-30171, CVE-2024-30172, CVE-2024-29857, CVE-2023-33201, CVE-2023-45287, CVE-2020-8694, CVE-2020-8695, CVE-2024-24557, CVE-2024-22201, CVE-2023-44487, CVE-2021-28169, CVE-2021-34428, CVE-2021-34429, CVE-2022-2047, CVE-2022-2048, CVE-2023-26048, CVE-2023-26049, CVE-2023-36478, CVE-2023-36479, CVE-2023-40167, CVE-2023-41900, CVE-2024-28757, CVE-2022-40674, CVE-2022-43680, CVE-2023-52425, CVE-2022-41912, CVE-2023-28119, CVE-2023-45683, CVE-2021-3538, CVE-2022-23806, CVE-2022-41716, CVE-2021-3115, CVE-2020-28367, CVE-2020-28366, CVE-2023-44487, CVE-2023-3978, CVE-2020-7711, CVE-2022-28948, CVE-2021-23463, CVE-2021-42392, CVE-2022-23221, CVE-2022-45868, CVE-2024-3651, CVE-2020-36518, CVE-2022-42003, CVE-2022-42004, CVE-2021-46877, CVE-2023-35116, CVE-2021-28168, CVE-2024-28180, CVE-2019-9893, CVE-2023-6378, CVE-2020-28362, CVE-2023-45288, CVE-2023-39325, CVE-2022-27664, CVE-2022-41717, CVE-2022-41723, CVE-2024-29025, CVE-2022-24823, CVE-2022-41881, CVE-2023-34462, CVE-2023-44487,CVE-2023-48795, CVE-2024-0727, CVE-2020-36242, CVE-2023-49083,CVE-2022-31197,CVE-2022-41946,CVE-2024-1597,CVE-2024-24786,CVE-2018-1000808, CVE-2018-1000807,CVE-2020-29651, CVE-2018-18074, CVE-2024-35195, CVE-2024-4032, CVE-2023-46218, CVE-2024-37891, CVE-2022-40897, CVE-2023-34453, CVE-2023-34454, CVE-2023-34455, CVE-2023-43642, CVE-2024-38808, CVE-2024-23944, CVE-2023-44981, CVE-2025-26477, CVE-2025-26478)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell ObjectScale 4.0 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 ObjectScale 4.0 (Versions 3.x.x through ECS 3.8.x)
Officially Acknowledged by the Vendor	Yess
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000300068/dsa-2025-097-security-update-for-dell-objectscale-4-0-multiple-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Out-of-bounds Write Vulnerability (CVE-2025-21785)
Description	Red Hat has released security updates addressing Out-of-bounds Write Vulnerability that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. **CVE-2025-21785** - In the Linux kernel, the following vulnerability has been resolved: arm64: cacheinfo: Avoid out-of-bounds write to cacheinfo array The loop that detects/populates cache information already has a bounds check on the array size but does not account for cache levels with separate data/instructions cache. Fix this by incrementing the index for any populated leaf (instead of any populated level). 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 8 • Red Hat Enterprise Linux for IBM z Systems 8 s390x • Red Hat Enterprise Linux for Power, little endian 8 ppc64le • Red Hat Enterprise Linux for ARM 64 8 aarch64 • Red Hat CodeReady Linux Builder for x86_64 8 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le • Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 • Red Hat Enterprise Linux for Real Time 8 x86_64 • Red Hat Enterprise Linux for Real Time for NFV 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:3260 • https://access.redhat.com/errata/RHSA-2025:3264

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20271, CVE-2024-20265, CVE-2023-20176, CVE-2024-20354)
Description	Cisco has released security updates addressing an multiple vulnerabilities that exists in Access Point Devices. **CVE-2024-20271** - A vulnerability in the IP packet processing of Cisco Access Point (AP) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. **CVE-2024-20265** - A vulnerability in the boot process of Cisco Access Point (AP) Software could allow an unauthenticated, physical attacker to bypass the Cisco Secure Boot functionality and load a software image that has been tampered with on an affected device. **CVE-2023-20176** - A vulnerability in the networking component of Cisco access point (AP) software could allow an unauthenticated, remote attacker to cause a temporary disruption of service. **CVE-2024-20354** - A vulnerability in the handling of encrypted wireless frames of Cisco Aironet Access Point (AP) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on the affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-ap-dos-h9TGGX6W.html • https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-ap-secureboot-bypass-zT5vJkSD.html • https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-click-ap-dos-wdcXkvnQ.html • https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-airo-ap-dos-PPPtcVW.html

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53140, CVE-2023-52880, CVE-2024-53104 ,CVE-2024-56672, CVE-2025-0927, CVE-2024-38558)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to compromise systems. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Ubuntu 14.04 ESM • Ubuntu 16.04 ESM • Ubuntu 18.04 ESM • Ubuntu 20.04 LTS • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/LSN-0110-1

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.