Advisory Alert

Alert Number: AAA20251217 **Date:** December 17, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Improper Handling Of Insufficient Entropy Vulnerability
Synology	**High**	Credential Disclosure Vulnerability

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53322, CVE-2023-53401, CVE-2023-53513, CVE-2025-38499, CVE-2025-39864, CVE-2025-39955, CVE-2025-39966, CVE-2025-39984, CVE-2025-40186)
Description	Red Hat 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. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 and 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 Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:23250 • https://access.redhat.com/errata/RHSA-2025:23427 • https://access.redhat.com/errata/RHSA-2025:23426 • https://access.redhat.com/errata/RHSA-2025:23423

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Improper Handling Of Insufficient Entropy Vulnerability (CVE-2025-62626)
Description	Dell has released security updates addressing an Improper Handling Of Insufficient Entropy Vulnerability that exists in certain AMD CPUs which affect Dell PowerEdge BIOS. **CVE-2025-62626** - Improper handling of insufficient entropy in the AMD CPUs could allow a local attacker to influence the values returned by the RDSEED instruction, potentially resulting in the consumption of insufficiently random values. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIOS Versions prior to 1.2.3 of PowerEdge XE9685L BIOS Versions prior to 1.5.3 of: • PowerEdge R6715 • PowerEdge R7715 • PowerEdge R6725 • PowerEdge R7725 • PowerEdge R7725xd • PowerEdge M7725 • PowerEdge XE7745
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000404520/dsa-2025-423-security-update-for-dell-amd-based-poweredge-server-vulnerability

Affected Product	**Synology**
Severity	**High**
Affected Vulnerability	Credential Disclosure Vulnerability (CVE-2025-14713)
Description	Synology has released security updates addressing a Credential Disclosure Vulnerability that exists in C2 Identity Edge Server. **CVE-2025-14713** - allows remote attackers to obtain user credentials from the edge server. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Versions prior to 1.76.0-0307 of: • C2 Identity Edge Server for DSM 7.3 • C2 Identity Edge Server for DSM 7.2.2 • C2 Identity Edge Server for DSM 7.2.1 • C2 Identity Edge Server for DSM 7.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_25_18

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.