Advisory Alert

Alert Number: AAA20241015 **Date:** October 15, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-39283, CVE-2024-22374)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in third-party products which in turn affect HPE products. These vulnerabilities could be exploited by malicious users to cause Denial of Service and Escalation of Privilege. **CVE-2024-39283 -** Incomplete filtering of special elements in Intel(R) TDX module software before version TDX_1.5.01.00.592 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE-2024-22374-** Insufficient control flow management for some Intel(R) Xeon Processors may allow an authenticated user to potentially enable denial of service via local access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant DX320 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DX360 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DX380 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DX380a Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DX4120 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DX560 Gen11 - Prior to v2.20_05-27-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04720en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04719en_us&docLocale=en_US

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47321, CVE-2021-47560, CVE-2022-34169, CVE-2022-36033, CVE-2023-1252, CVE-2023-51775, CVE-2024-35884, CVE-2024-36025, CVE-2024-36952, CVE-2024-38558, CVE-2024-39476, CVE-2024-4029, CVE-2024-4068, CVE-2024-40998, CVE-2024-41040, CVE-2024-42284, CVE-2024-47561)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Remote Code Execution, Denial Of Service, Cross-site scripting, Use-After-Free Condition, NULL pointer dereference Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:8107 • https://access.redhat.com/errata/RHSA-2024:8093 • https://access.redhat.com/errata/RHSA-2024:8080 • https://access.redhat.com/errata/RHSA-2024:8077 • https://access.redhat.com/errata/RHSA-2024:8076 • https://access.redhat.com/errata/RHSA-2024:8075

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.