Advisory Alert

Alert Number: **AAA20240124** **Date:** **January 24, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
HPE	**High ,** **Medium**	Multiple Vulnerabilities
Dell	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-2163, CVE-2023-4622, CVE-2023-4623, CVE-2023-39191, CVE-2023-45871, CVE-2023-3611, CVE-2023-3812, CVE-2023-5178, CVE-2023-31436, CVE-2023-42753)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to denial of service, out-of-bounds write, use after free, slab-out-of-bound access due to integer underflow Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Workstation 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0381 https://access.redhat.com/errata/RHSA-2024:0378 https://access.redhat.com/errata/RHSA-2024:0376 https://access.redhat.com/errata/RHSA-2024:0371 https://access.redhat.com/errata/RHSA-2024:0346 https://access.redhat.com/errata/RHSA-2024:0340

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Remote Code Execution, Denial of Service, Disclosure of Information HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	HPE Superdome Flex Server - Prior to v3.90.18 HPE Superdome Flex 280 Server - Prior to v1.70.14 HPE Compute Scale-up Server 3200 - Prior to v1.10.342
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04576en_us

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-29081)
Description	Dell has released a security update addressing a denial-of-service vulnerability in the InstallShield third-party component, which affects their Dell Encryption, Dell Endpoint Security Suite Enterprise, and Dell Security Management which could be exploited by malicious users to compromise the affected system during installation. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	Dell Encryption Versions prior to 11.9.0 Dell Endpoint Security Suite Enterprise Versions prior to 11.9.0 Dell Security Management Server (Windows) Versions prior to 11.9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000215214/dsa-2023-235-dell

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.