Advisory Alert

Alert Number: AAA20240130 **Date:** January 30, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Dell	**Medium**	Encryption Vulnerability

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46589, CVE-2023-2163, CVE-2023-3611, CVE-2023-3812, CVE-2023-4622, CVE-2023-4623, CVE-2023-5178, CVE-2023-31436, CVE-2023-45871)
Description	Red Hat has released security updates addressing Multiple Vulnerabilities that exist in their products. An attacker could exploit these vulnerabilities to cause Out-of-bounds write, Use after free condition, Bugs for oversize packets, HTTP request smuggling. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 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 Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0539 https://access.redhat.com/errata/RHSA-2024:0554

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Encryption Vulnerability (CVE-2023-48795)
Description	Dell has released security updates addressing an Encryption Vulnerability that exists in OpenSSH third party component that affects Dell iDRAC. Dell recommends to apply the workarounds and mitigations at your earliest to avoid issues.
Affected Products	iDRAC 9 iDRAC 8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000221558/dsa-2024-021-idrac-8-and-idrac-9-security-update-for-cve-2023-48795

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.