Advisory Alert

Alert Number: AAA20230526 **Date:** May 26, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Improper handling Vulnerability
NetApp	**Medium**	Information Disclosure Vulnerability

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Improper handling Vulnerability (CVE-2023-24540)
Description	Redhat has released security update addressing an Improper handling vulnerability that exists in their products. **CVE-2023-24540**- The vulnerability in question involves improper handling of JavaScript whitespace in the html/template package of the Go programming language. Redhat 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 x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux Server - AUS 8.8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:3319

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2023-27311)
Description	Netapp has released security update addressing an Information disclosure vulnerability that exists in their products. A vulnerability has been identified in NetApp Blue XP Connector versions prior to 3.9.25, which exposes sensitive information through a directory listing. Successful exploitation of this vulnerability could result in the disclosure of sensitive information. Netapp recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	NetApp BlueXP 3.9.25
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20230525-0001/

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.