Advisory Alert

Alert Number: AAA20231006 **Date:** October 6, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
HP	**Medium**	Privilege escalation vulnerability
F5	**Medium**	Stored cross-site scripting vulnerability

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-25883, CVE-2023-3171, CVE-2023-4061, CVE-2023-26136, CVE-2023-26464, CVE-2023-33201, CVE-2023-34462)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to denial of service, heap exhaustion, prototype pollution Redhat recommends to apply the necessary security updates at earliest to avoid issues
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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:5484 https://access.redhat.com/errata/RHSA-2023:5485 https://access.redhat.com/errata/RHSA-2023:5486 https://access.redhat.com/errata/RHSA-2023:5488

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-38457, CVE-2022-40133, CVE-2023-1192, CVE-2023-1859, CVE-2023-2007, CVE-2023-20588, CVE-2023-2177, CVE-2023-34319, CVE-2023-3610, CVE-2023-37453, CVE-2023-3772, CVE-2023-3863, CVE-2023-40283, CVE-2023-4128, CVE-2023-4133, CVE-2023-4134, CVE-2023-4147, CVE-2023-4194, CVE-2023-4273, CVE-2023-4387, CVE-2023-4459, CVE-2023-4563, CVE-2023-4569, CVE-2023-4881)
Description	SUSE has released a security update addressing multiple vulnerabilities exist in in their products. Successful exploitation of these vulnerabilities could lead to use-after-free, privilege escalation, NULL pointer dereference SUSE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Real Time Module 15-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233988-1/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing multiple vulnerabilities that exists in multiple third party components used in Dell PowerStore. Successful exploitation of these vulnerabilities could lead malicious users to compromise the affected system. Dell recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Dell PowerStore 1000T, 1200T, 3000T, 3200T, 5000T, 500T, 5200T, 7000T, 9000T, 9200T
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000218046/dsa-2023-366-dell-powerstore-family-security-update-for-multiple-vulnerabilities

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Privilege escalation vulnerability (CVE-2022-26006)
Description	HPE has released a security update addressing a privilege escalation vulnerability in Apollo products for certain Intel processors that could be locally exploited due to improper input validation in the BIOS firmware. HPE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	HPE ProLiant XL170r Gen9 Server - Prior to v3.04_08-04-2022 HPE ProLiant XL190r Gen9 Server - Prior to v3.04_08-04-2022 HPE ProLiant XL230a Gen9 Server - Prior to v3.04_08-04-2022 HPE ProLiant XL230b Gen9 Server - Prior to v3.04_08-04-2022 HPE ProLiant XL250a Gen9 Server - Prior to v3.04_08-04-2022 HPE ProLiant XL270d Gen9 Accelerator Tray 2U Configure-to-order Server - Prior to v3.04_08-04-2022 HPE ProLiant XL730f Gen9 Server - Prior to v3.04_08-04-2022 HPE ProLiant XL740f Gen9 Server - Prior to v3.04_08-04-2022 HPE ProLiant XL750f Gen9 Server - Prior to v3.04_08-04-2022
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04374en_us

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Stored cross-site scripting vulnerability (CVE-2022-27878)
Description	F5 has released a security update addressing a stored cross-site scripting vulnerability exist in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. F5 recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	BIG-IP (all modules) 16.0.0 - 16.1.3 BIG-IP (all modules) 15.1.0 - 15.1.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K92807525

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.