Advisory Alert

Alert Number: AAA20241001 **Date:** October 1, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Denial of Service Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
NetApp	**Medium**	Multiple Vulnerabilities
F5	**Medium**	HTML Attribute Injection Vulnerability
IBM	**Medium**	Stored Cross-site Scripting Vulnerability

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Denial of Service Vulnerabilities (CVE-2012-0876, CVE-2021-22925, CVE-2021-3520, CVE-2022-43680, CVE-2023-28322, CVE-2023-3446, CVE-2023-38546, CVE-2023-39615, CVE-2023-46218, CVE-2023-48795, CVE-2023-52425, CVE-2023-52426, CVE-2023-5363, CVE-2023-5678, CVE-2023-6237, CVE-2024-0727, CVE-2024-28757, CVE-2024-31497)
Description	HPE has released security updates addressing multiple Denial of Service vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• HPE NonStop QRSTR software T1137 - T1137V01, T1137V01^AAA to AAD • HPE BackBox Software T0954 - T0954V04, T0954V04^AAA to AAW, T0954V04^AAA to AAV - T0954V04^AAA to AAW, T0954V04^AAA to AAV
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbns04707en_us&docLocale=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0854, CVE-2022-20368, CVE-2022-28748, CVE-2022-2964, CVE-2022-48686, CVE-2022-48791, CVE-2022-48802, CVE-2022-48805, CVE-2022-48839, CVE-2022-48853, CVE-2022-48872, CVE-2022-48873, CVE-2022-48901, CVE-2022-48912, CVE-2022-48919, CVE-2022-48925, CVE-2023-1582, CVE-2023-2176, CVE-2023-52854, CVE-2024-26583, CVE-2024-26584, CVE-2024-26800, CVE-2024-41011, CVE-2024-41062, CVE-2024-42077, CVE-2024-42232, CVE-2024-42271, CVE-2024-43861, CVE-2024-43882, CVE-2024-43883, CVE-2024-44947)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Availability Extension 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Live Patching 15-SP2 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server for SAP Applications 15 SP2 SUSE Manager Proxy 4.1 SUSE Manager Retail Branch Server 4.1 SUSE Manager Server 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20243499-1/

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5678, CVE-2023-51384, CVE-2023-51385, CVE-2023-48795, CVE-2024-0727, CVE-2024-5642)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Disclosure of Sensitive Information and Addition or Modification of Data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetApp Manageability SDK E-Series SANtricity OS Controller Software 11.x Active IQ Unified Manager for VMware vSphere Active IQ Unified Manager for Microsoft Windows ONTAP 9 (formerly Clustered Data ONTAP) FAS/AFF Baseboard Management Controller (BMC) - A900/9500 FAS/AFF Baseboard Management Controller (BMC) - FAS2820 StorageGRID (formerly StorageGRID Webscale)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20231130-0010/ • https://security.netapp.com/advisory/ntap-20240105-0005/ • https://security.netapp.com/advisory/ntap-20240105-0004/ • https://security.netapp.com/advisory/ntap-20240208-0006/ • https://security.netapp.com/advisory/ntap-20240726-0005/

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	HTML Attribute Injection Vulnerability (CVE-2024-22195)
Description	F5 has released security updates addressing an HTML Attribute Injection Vulnerability that exists in their products. **CVE-2024-22195 -** Jinja is an extensible templating engine. Special placeholders in the template allow writing code similar to Python syntax. It is possible to inject arbitrary HTML attributes into the rendered HTML template, potentially leading to Cross-Site Scripting (XSS). The Jinja `xmlattr` filter can be abused to inject arbitrary HTML attribute keys and values, bypassing the auto escaping mechanism and potentially leading to XSS. It may also be possible to bypass attribute validation checks if they are blacklist-based. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Traffix SDC - 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000141253

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Stored Cross-site Scripting Vulnerability (CVE-2024-45073)
Description	IBM has released security updates addressing a Stored Cross-site Scripting Vulnerability that exists in their products. **CVE-2024-45073 -** IBM WebSphere Application Server is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server - Versions 8.5, 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7171755

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.