Advisory Alert

Alert Number: AAA20230802 **Date:** August 2, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
HPE	**High**	Authenticated Command Injection Vulnerability
Synology	**High**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
OpenSSL	**Low**	Resource management Vulnerability

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31425, CVE-2023-31426, CVE-2023-31427, CVE-2023-31428, CVE-2023-31429, CVE-2023-31430, CVE-2023-31431, CVE-2023-31432, CVE-2023-31926, CVE-2023-31927, CVE-2022-0778, CVE-2021-41617, CVE-2018-7738, CVE-2022-0155, CVE-2018-25032, CVE-2022-44792, CVE-2021-4145, CVE-2021-39275, CVE-2020-14145, CVE-2019-0220, CVE-2018-0739, CVE-2021-3800, CVE-2022-24448, CVE-2022-23219, CVE-2021-45485, CVE-2021-45486, CVE-2021-0146, CVE-2022-3786, CVE-2022-3602, CVE-2022-28614, CVE-2022-28615, CVE-2022-0322, CVE-2020-36557, CVE-2020-36558, CVE-2022-29154, CVE-2022-2097, CVE-2011-4917, CVE-2022-2068, CVE-2020-15861, CVE-2012-0060, CVE-2014-2524, CVE-2022-25313, CVE-2021-20193, CVE-2022-25236, CVE-2022-25235, CVE-2018-14348, CVE-2018-14404, CVE-2023-31928)
Description	HPE has released security update addressing multiple Vulnerabilities in their products. If exploited, the most severe vulnerabilities could lead to Denial of Service (DoS), Privilege Escalation , Sensitive Information Disclosure, Buffer Overflow HPE highly recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	HPE Fibre Channel and SAN Switches with Brocade Fabric OS (FOS)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04494en_us

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Authenticated Command Injection Vulnerability (CVE-2023-3718)
Description	HPE has released a security update addressing An authenticated command injection vulnerability that exists in the AOS-CX command line interface. Successful exploitation of this vulnerability could lead to the execution of arbitrary commands on the underlying operating system as a privileged user on the affected switch. HPE recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Aruba CX 10000 Switch Series Aruba CX 9300 Switch Series Aruba CX 8400 Switch Series Aruba CX 8360 Switch Series Aruba CX 8325 Switch Series Aruba CX 8320 Switch Series Aruba CX 6400 Switch Series Aruba CX 6300 Switch Series Aruba CX 6200 Switch Series Aruba CX 6100 Switch Series Aruba CX 6000 Switch Series Aruba CX 4100i Switch Series Software Branch Versions: • AOS-CX 10.11.xxxx: 10.11.1010 and below. • AOS-CX 10.10.xxxx: 10.10.1050 and below.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04498en_us

Affected Product	**Synology**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities
Description	Synology has released a security update addressing Multiple vulnerabilities in their Synology Router Manager. If exploited , most severe vulnerabilities could allow remote attackers to read specific files, obtain sensitive information, and inject arbitrary web script or HTML, man-in-the-middle attackers to bypass security constraint, and remote authenticated users to execute arbitrary commands and conduct denial-of-service attacks Synology recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Synology Router Manager (SRM) version 1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_23_10

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-24736, CVE-2022-41723, CVE-2022-4304, CVE-2022-45869, CVE-2023-0215, CVE-2023-0286, CVE-2023-0458, CVE-2023-1667, CVE-2023-1998, CVE-2023-2283, CVE-2023-24329, CVE-2023-24540, CVE-2023-26604, CVE-2023-2828, CVE-2023-3089, CVE-2023-3090, CVE-2023-35788)
Description	Redhat has released security updates addressing multiple Vulnerabilities in their products. If exploited, the most severe vulnerabilities could lead to privilege escalation, compromised Integrity, authorization bypass, NULL pointer dereference. Redhat recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Container Native Virtualization 4.12 for RHEL 7 x86_64 Red Hat Container Native Virtualization 4.12 for RHEL 8 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 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 9.2 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:4421 https://access.redhat.com/errata/RHSA-2023:4420 https://access.redhat.com/errata/RHSA-2023:4377 https://access.redhat.com/errata/RHSA-2023:4378 https://access.redhat.com/errata/RHSA-2023:4380

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-2002, CVE-2023-35788, CVE-2023-2235, CVE-2023-3159, CVE-2023-33952)
Description	Suse has released security updates addressing Multiple vulnerabilities in their products. If exploited, most severe vulnerabilities could allow out-of-bounds writes, use-after-free conditions, unauthorized execution of management commands, and Privilege escalation. Suse recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.4, 15.5 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP2, SP3, SP4, SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP2, SP3, SP4, SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP2, SP3, SP4, SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP2, SP3, SP4, SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233041-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233055-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233036-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233035-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233046-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233069-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233063-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233079-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233076-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233075-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233073-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233083-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233081-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233111-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233107-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233104-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233116-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233115-1/

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Resource management Vulnerability (CVE-2023-3817)
Description	OpenSSL has released a security update addressing Resource management error exists due to improper management of internal resources within the application when checking the long DH keys. By exploiting this vulnerability a remote attacker can pass specially crafted data to the application and perform a denial of service. OpenSSL recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	OpenSSL 3.1, 3.0, 1.1.1 and 1.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20230731.txt

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.