Advisory Alert

Alert Number: AAA20230322 **Date:** March 22, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Authenticated Remote Code Execution vulnerability
Suse	**High**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Authenticated Remote Code Execution vulnerability (CVE-2023-1168)
Description	HPE has released a security update addressing a Remote Code Execution vulnerability that exists in their products. Remote privileged user can send specially crafted data to the application and execute arbitrary OS commands on the system due to improper input validation in the AOS-CX network analytics engine. HPE recommends to apply necessary security fixes at 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 6200F Switch Series AOS-CX 10.10.xxxx: 10.10.1020 and below. AOS-CX 10.09.xxxx: 10.09.1020 and below. AOS-CX 10.08.xxxx: 10.08.1070 and below. AOS-CX 10.06.xxxx: 10.06.0230 and below.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04460en_us

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-4203, CVE-2022-2991, CVE-2022-36280, CVE-2022-38096, CVE-2022-4129, CVE-2023-0045, CVE-2023-0590, CVE-2023-23559, CVE-2023-26545)
Description	Suse has released a security update to address multiple vulnerabilities that exist in their products. These vulnerabilities allows an attacker to cause denial of service, use-after-free read condition, heap-based overflow, NULL-pointer dereference. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Availability Extension 12 SP4 SUSE Linux Enterprise High Performance Computing 12 SP4 SUSE Linux Enterprise Live Patching 12-SP4 SUSE Linux Enterprise Server 12 SP4 SUSE Linux Enterprise Server 12 SP4 ESPOS 12-SP4 SUSE Linux Enterprise Server 12 SP4 LTSS 12-SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP4 SUSE OpenStack Cloud 9 SUSE OpenStack Cloud Crowbar 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20230852-1/

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2012-6708, CVE-2015-9251, CVE-2018-15494, CVE-2019-11358, CVE-2020-11022, CVE-2020-11023, CVE-2020-7656, CVE-2022-43863, CVE-2023-26283)
Description	IBM has released security updates to address multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to privilege escalation, sensitive information disclosure and cross-site scripting. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Application Server 9.0 WebSphere Extreme Scale 8.6.1.0 - 8.6.1.5 IBM QRadar SIEM 7.5.0 - 7.5.0 UP4 IBM QRadar SIEM 7.4.3 GA - 7.4.3 FP8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6964836 https://www.ibm.com/support/pages/node/6964844 https://www.ibm.com/support/pages/node/6964862

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.