Advisory Alert

Alert Number: **AAA20240620** **Date:** **June 20, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Trellix	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High,** **Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37897, CVE-2022-37898, CVE-2022-37899, CVE-2022-37900, CVE-2022-37901, CVE-2022-37902, CVE-2022-37903, CVE-2022-37904, CVE-2022-37905, CVE-2022-37906, CVE-2022-37907, CVE-2022-37908, CVE-2022-37909, CVE-2022-37910, CVE-2022-37911, CVE-2022-37912)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Arbitrary Code Execution, Arbitrary Command Execution, Arbitrary File Deletion, Denial of Service (DoS), Disclosure of Sensitive Information, unauthorized modification, XML External Entity (XXE). HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Aruba Mobility Conductor (formerly Mobility Master) Aruba Mobility Controllers WLAN Gateways and SD-WAN Gateways managed by Aruba Central Affected Software Versions: • ArubaOS 6.5.4.x : ArubaOS 6.5.4.22 and below • ArubaOS 8.6.x.x : ArubaOS 8.6.0.17 and below • ArubaOS 8.7.x.x : ArubaOS 8.7.1.9 and below • ArubaOS 10.3.x.x : 10.3.0.0 • SD-WAN 8.7.0.0-2.3.0.x : 8.7.0.0-2.3.0.6 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04381en_us&docLocale=en_US

Affected Product	**Trellix**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-5671, CVE-2024-5731)
Description	Trellix has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-5671 -** Insecure deserialization in some IPS Manager workflows allows unauthenticated remote attackers to execute arbitrary code and access the vulnerable Trellix IPS Manager. **CVE-2024-5731 -** This vulnerability in the IPS Manager, Central Manager, and Local Manager communication workflow allows an attacker to manipulate the destination of the request by altering the IP Address parameter in the request. Additionally, the request parameter contains an encoded string with the username and password, which can be decoded to obtain the original string. Trellix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IPS Manager and IPS Central Manager 11.1.7.84 Prior Version.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.trellix.com/bundle/intrusion-prevention-system-11.1.x-manager-ns-series-release-notes/page/UUID-18de5423-4520-d400-f539-fc3184256955.html

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-48687, CVE-2023-52628, CVE-2024-26852, CVE-2022-48651 CVE-2023-52340, CVE-2023-52502, CVE-2023-6546, CVE-2024-26585, CVE-2024-26610, CVE-2024-26622, CVE-2024-26766, CVE-2023-6931)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Use After Free Condition, Out of Bound Reads, Privilege Escalation, Denial of Service. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Opens USE 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242091-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242092-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242094-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242099-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242100-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242101-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242096-1

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20919, CVE-2024-20926, CVE-2024-20945, CVE-2023-33850, CVE-2024-23672, CVE-2024-24549)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of Service, Sensitive Information disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Virtualize - 8.4, 8.5, 8.6 Versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7156536 • https://www.ibm.com/support/pages/node/7156538

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.