Advisory Alert

Alert Number: AAA20250317 **Date:** March 17, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Remote Command Execution Vulnerabilities
NetApp	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
HPE	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Remote Command Execution Vulnerabilities (CVE-2024-42393, CVE-2024-42394, CVE-2024-42395)
Description	HPE has released security updates addressing Multiple Remote Command Execution Vulnerabilities that exist in Aruba Access Points. **CVE-2024-42393, CVE-2024-42394** - There are vulnerabilities in the Soft AP Daemon Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE-2024-42395 -** There is a vulnerability in the AP Certificate Management Service which could allow a threat actor to execute an unauthenticated RCE attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. HPE advises to Upgrade the Access Point at your earliest to protect systems from potential threats.
Affected Products	AOS-8 Instant 8.12.x.x: 8.12.0.2 and above AOS-8 Instant 8.10.x.x: 8.10.0.13 and above
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-25291, CVE-2025-25292)
Description	NetApp has released security updates addressing Multiple Vulnerabilities that exist in their Product. **CVE-2025-25291, CVE-2025-25292** - Multiple NetApp products incorporate Ruby SAML. Ruby SAML versions prior to 1.12.4 and 1.13.0 prior to 1.18.0 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information or addition or modification of data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	StorageGRID (formerly StorageGRID Webscale)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250314-0010/ • https://security.netapp.com/advisory/ntap-20250314-0009/

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their SUSE Linux Enterprise 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 Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro for Rancher 5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20250867-1/

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51385, CVE-2023-48795, CVE-2024-42396, CVE-2024-42397, CVE-2024-42398, CVE-2024-42399, CVE-2024-42400)
Description	HPE 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. **CVE-2023-51385 -** In OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name. The impact of this vulnerability on InstantOS 8.x and ArubaOS 10.x running on HPE Aruba Networking Access Points has not been confirmed, but the version of OpenSSH has been upgraded for mitigation. **CVE-2023-48795 -** The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. The impact of this vulnerability on HPE Aruba Networking Access Points has not been confirmed, but the version of OpenSSH in InstantOS and ArubaOS 10.x software has been upgraded for mitigation. **CVE-2024-42396, CVE-2024-42397** - Multiple unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the AP Certificate Management daemon accessed via the PAPI protocol. Successful exploitation of these vulnerabilities results in the ability to interrupt the normal operation of the affected Access Point. **CVE-2024-42398, CVE-2024-42399, CVE-2024-42400** - Multiple unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the Soft AP daemon accessed via the PAPI protocol. Successful exploitation of these vulnerabilities results in the ability to interrupt the normal operation of the affected Access Point. HPE advises to Upgrade the Access Point at your earliest to protect systems from potential threats.
Affected Products	AOS-10 AP 10.6.x.x: 10.6.0.0 and below AOS-10 AP 10.4.x.x: 10.4.1.3 and below AOS-8 Instant 8.12.x.x: 8.12.0.1 and below AOS-8 Instant 8.10.x.x: 8.10.0.12 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US

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.