Advisory Alert

Alert Number: **AAA20240925** **Date:** **September 25, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Arbitrary Command Execution Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High,** **Medium**	Multiple Vulnerabilities
IBM	**High,** **Medium,** **Low**	Multiple Vulnerabilities
Citrix	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Arbitrary Command Execution Vulnerabilities (CVE-2024-42505, CVE-2024-42506, CVE-2024-42507)
Description	HPE has released security updates addressing Multiple Arbitrary Command Execution Vulnerabilities that exist in their products. Command injection vulnerabilities in the underlying CLI service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking • Aruba Access Points running Instant AOS-8 and AOS 10 Affected Software Version(s): • AOS-10.6.x.x: 10.6.0.2 and below • AOS-10.4.x.x: 10.4.1.3 and below • Instant AOS-8.12.x.x: 8.12.0.1 and below • Instant AOS-8.10.x.x: 8.10.0.13 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04712en_us&docLocale=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Use After Free, Memory Leak, Integer Overflow, Memory Corruption. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP6 Development Tools Module 15-SP6 Legacy Module 15-SP6 OpenSUSE Leap 15.4, 15.5, 15.6 SUSE Linux Enterprise Desktop 15 SP4 LTSS 15-SP4, 15 SP6 SUSE Linux Enterprise High Availability Extension 15 SP4, 15 SP6 SUSE Linux Enterprise High Performance Computing 15 SP4, 15 SP5, ESPOS 15 SP4, LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5, 15-SP6 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server 15 SP4, 15 SP4 LTSS 15-SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Workstation Extension 15 SP6 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243361-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243383-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243387-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243395-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243398-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243399-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243403-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243405-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243408-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243425-1

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38709, CVE-2024-38472, CVE-2024-40898)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-38709 -** A flaw was found in httpd. The response headers are not sanitized before an HTTP response is sent when a malicious backend can insert a Content-Type, Content-Encoding, or some other headers, resulting in an HTTP response splitting. **CVE-2024-38472 -** A flaw was found in httpd on Windows systems. This issue potentially allows NTLM hashes to be leaked to a malicious server via Server-side request forgery (SSRF) and malicious requests or content. **CVE-2024-40898 -** A flaw was found in HTTPd on Windows systems. This issue potentially allows NTLM hashes to be leaked via mod_rewrite in server/vhost context to a malicious server via Server-side request forgery (SSRF) and malicious requests or content. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services 1 for RHEL 7 x86_64 Red Hat JBoss Core Services Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:6928 • https://access.redhat.com/errata/RHSA-2024:6927

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1073, CVE-2023-45871, CVE-2023-6356, CVE-2023-6535, CVE-2023-6536, CVE-2023-1206, CVE-2023-5178, CVE-2024-21131)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Storage Virtualize. These vulnerabilities could be exploited by malicious users to cause Denial Of Service, Privilege Escalation, Arbitrary Code Execution and low Integrity Impact. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Virtualize - Versions 8.4, 8.5, 8.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7161786 • https://www.ibm.com/support/pages/node/7166856

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45817, CVE-2022-24805, CVE-2022-24809)
Description	Citrix has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could allow a malicious administrator of a guest VM to cause the host to crash or become unresponsive. Additionally, an attacker on the management network could cause the XenServer host's SNMP service to crash or become unresponsive. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Citrix Hypervisor 8.2 CU1 LTSR XenServer 8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/s/article/CTX691646-xenserver-and-citrix-hypervisor-security-update-for-cve202445817?language=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.