Advisory Alert

Alert Number: AAA20250120 **Date:** January 20, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Palo Alto	**Medium**	Privilege Escalation Vulnerability

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27316, CVE-2024-24795, CVE-2023-38709, CVE-2024-38476, CVE-2024-39573, CVE-2024-38474, CVE-2024-38473, CVE-2024-39884, CVE-2024-40725, CVE-2024-36387, CVE-2024-38475, CVE-2024-38477)
Description	HPE has released security updates to address multiple vulnerabilities in HP-UX Apache-based Web Server. These vulnerabilities could be exploited locally/remotely to perform HTTP request smuggling, null pointer dereference, memory exhaustion, SSRF, disclosure of information, code execution or bypass authentication restriction. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HP-UX Apache-based Web Server Prior to B.2.4.62.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04773en_us&docLocale=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52752, CVE-2024-50264, CVE-2022-48956, CVE-2024-43861, CVE-2024-35949, CVE-2024-40909, CVE-2024-40954)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to memory leak, use after free condition. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap: 15.6, 15.5, 15.4 SUSE Linux Enterprise Live Patching: 15-SP6, 15-SP5, 15-SP4, 12-SP5 SUSE Linux Enterprise Real Time: 15 SP6, 15 SP5, 15 SP4 SUSE Linux Enterprise Server: 15 SP6, 15 SP5, 15 SP4, 12 SP5 SUSE Linux Enterprise Server for SAP Applications: 15 SP6, 15 SP5, 15 SP4, 12 SP5 SUSE Linux Enterprise High Performance Computing: 15 SP5, 15 SP4, 12 SP5 SUSE Linux Enterprise Micro: 5.5, 5.4, 5.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20250179-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250173-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250177-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250172-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250168-1/

Affected Product	**Palo Alto**
Severity	**Medium** - Initial release date 26th November 2024 **(AAA20241126)**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2024-5921)
Description	Palo Alto has released security updates addressing a Privilege Escalation Vulnerability that exists in their products. **CVE-2024-5921** - An insufficient certification validation issue in the Palo Alto Networks GlobalProtect app enables attackers to connect the GlobalProtect app to arbitrary servers. This can enable an attacker to install malicious root certificates on the endpoint and subsequently install malicious software signed by the malicious root certificates on that endpoint. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• GlobalProtect App 6.3 Versions Below 6.3.2 on Windows Versions Below 6.3.2 on macOS • GlobalProtect App 6.2 Versions Below 6.2.1-HF2 on Linux Versions Below 6.2.6 on Windows Versions Below 6.2.6 -c857 on macOS • GlobalProtect App 6.1 All Versions on Windows, macOS, Linux, Android Versions Below 6.1.7 on iOS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-5921

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.