Advisory Alert

Alert Number: AAA20241209 **Date:** December 9, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
QNAP	**High**, **Medium**	Multiple Vulnerabilities
Palo Alto	**Medium**	Privilege Escalation Vulnerability
F5	**Medium**	Information Disclosure Vulnerability
IBM	**Medium** , **Low**	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-46955, CVE-2021-47291, CVE-2021-47378, CVE-2021-47383, CVE-2021-47402, CVE-2021-47517, CVE-2021-47598, CVE-2021-47600, CVE-2022-48651, CVE-2022-48662, CVE-2023-1829, CVE-2023-52340, CVE-2023-52502, CVE-2023-52752, CVE-2023-52846, CVE-2023-6531, CVE-2023-6546, CVE-2024-23307, CVE-2024-26585, CVE-2024-26610, CVE-2024-26622, CVE-2024-26766, CVE-2024-26828, CVE-2024-26852, CVE-2024-26923, CVE-2024-26930, CVE-2024-27398, CVE-2024-35817, CVE-2024-35861, CVE-2024-35862, CVE-2024-35863, CVE-2024-35864, CVE-2024-35867, CVE-2024-35905, CVE-2024-35949, CVE-2024-35950, CVE-2024-36899, CVE-2024-36904, CVE-2024-36964, CVE-2024-40909, CVE-2024-40954, CVE-2024-41059, CVE-2024-43861)
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap Versions: 15.3, 15.4, 15.5 SUSE Linux Enterprise High Performance Computing (HPC): Versions 12 SP5, 15 SP2, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching: Versions 12-SP5, 15-SP2, 15-SP3, 15-SP4, 15-SP5 SUSE Linux Enterprise Micro: Versions 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time: Versions 15 SP4, 15 SP5 SUSE Linux Enterprise Server: Versions 12 SP5, 15 SP2, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications: Versions 12 SP5, 15 SP2, 15 SP3, 15 SP4, 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20244256-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244250-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244249-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244248-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244247-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244246-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244243-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244242-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244241-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244240-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244239-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244237-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244236-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244235-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244234-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244230-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244231-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244228-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244227-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20244226-1

Affected Product	**QNAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50404, CVE-2024-48859, CVE-2024-48865, CVE-2024-48866, CVE-2024-48867, CVE-2024-48868, CVE-2024-50393, CVE-2024-50402, CVE-2024-50403, CVE-2024-48863)
Description	QNAP has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Arbitrary Command Execution, Privilege Escalation, Modification of Application Data, Information Disclosure QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	License Center 1.9.x Versions below 1.9.43 QTS 5.1.x Versions below 5.1.9.2954 build 20241120 QTS 5.2.x Versions below 5.2.2.2950 build 20241114 QuTS hero h5.1.x Versions below h5.1.9.2954 build 20241120 QuTS hero h5.2.x Versions below h5.2.2.2952 build 20241116 Qsync Central Versions below 4.4.0.16_20240819 (2024/08/19)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-24-50 • https://www.qnap.com/en/security-advisory/qsa-24-49 • https://www.qnap.com/en/security-advisory/qsa-24-48

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-HF on Linux Versions Below 6.2.6 on Windows Versions Below 6.2.6-HF on macOS • GlobalProtect App 6.1 All Versions on Windows, macOS, Linux, Android Versions Below 6.1.7 on iOS • GlobalProtect UWP App All Versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-5921

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2023-43753)
Description	F5 has released security updates addressing a vulnerability involving improper condition checks in certain Intel processors with Intel SGX. If exploited, a privileged user could potentially enable information disclosure via local access. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS-A: Versions 1.x (1.7.0 - 1.8.0, 1.5.1 - 1.5.2) running on Intel CPUs in the r5600, r5800, r5900, and r10900 platforms. F5OS-C: Versions 1.x (1.6.0 - 1.6.2) running on CPUs in the VELOS BX520 platform.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000148896

Affected Product	**IBM**
Severity	**Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47107, CVE-2024-21235, CVE-2024-21217, CVE-2024-21210, CVE-2024-21208, CVE-2024-10917)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to cause Credential Disclosure, Denial Of Service, Unauthorized Access To Data IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM Versions 7.5 - 7.5.0 UP10 IF01 WebSphere Service Registry and Repository Version 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7178104 • https://www.ibm.com/support/pages/node/7178094

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.