Advisory Alert

Alert Number: AAA20260106 **Date:** January 6, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-24519, CVE-2025-26694, CVE-2025-27710, CVE-2025-27713, CVE-2025-30509, CVE-2025-31937, CVE-2025-32088, CVE-2025-32446, CVE-2025-32732, CVE-2025-33000)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in Intel QuickAssist Technology (QAT) software drivers for Windows used in several HPE server products. These vulnerabilities could be locally exploited by malicious users to cause an escalation of privilege, disclosure of sensitive information, or a Denial of Service. HPE advises applying these security fixes at your earliest convenience to protect against potential threats and ensure system stability.
Affected Products	(QAT software driver version prior to v2.6.0) • HPE ProLiant XD230 • HPE ProLiant DL110 Gen11 • HPE ProLiant DL320 Gen12 / Gen11 • HPE ProLiant DL340 Gen12 • HPE ProLiant DL360 Gen12 / Gen11 • HPE ProLiant DL380 Gen12 / Gen11 • HPE ProLiant DL380a Gen12 / Gen11 • HPE ProLiant DL560 Gen11 • HPE ProLiant DL580 Gen12 • HPE ProLiant ML110 Gen11 • HPE ProLiant ML350 Gen12 / Gen11 • HPE Compute Edge Server e930t • HPE Compute Scale-up Server 3200 • HPE Alletra Storage Server 4210 • HPE Synergy 480 Gen12 Compute Module
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesb3p04984en_us&docLocale=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50280, CVE-2023-53676, CVE-2025-39967, CVE-2025-40040, CVE-2025-40048, CVE-2025-40121, CVE-2025-40154, CVE-2025-40204)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in the Linux kernel for their products. These vulnerabilities could be exploited by malicious users to cause a Denial of Service, unauthorized disclosure of sensitive information, or the modification of system data and memory through buffer overflows and integer overflows. SUSE advises applying these security fixes at your earliest convenience to protect against potential threats and ensure system stability.
Affected Products	openSUSE Leap 15.4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP4 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Proxy 4.3 LTS SUSE Manager Retail Branch Server 4.3 SUSE Manager Retail Branch Server 4.3 LTS SUSE Manager Server 4.3 SUSE Manager Server 4.3 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20260029-1/

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.