Advisory Alert

Alert Number: AAA20260216 **Date:** February 16, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49604, CVE-2022-49943, CVE-2022-49980, CVE-2022-50232, CVE-2022-50697, CVE-2023-52433, CVE-2023-52874, CVE-2023-52923, CVE-2023-53178, CVE-2023-53407, CVE-2023-53412, CVE-2023-53417, CVE-2023-53418, CVE-2023-53714, CVE-2023-54142, CVE-2023-54243, CVE-2024-26581, CVE-2024-26661, CVE-2024-26832, CVE-2024-50143, CVE-2024-54031, CVE-2025-21658, CVE-2025-21760, CVE-2025-21764, CVE-2025-21765, CVE-2025-21766, CVE-2025-38068, CVE-2025-38129, CVE-2025-38159, CVE-2025-38375, CVE-2025-38563, CVE-2025-38565, CVE-2025-38684, CVE-2025-40044, CVE-2025-40139, CVE-2025-40257, CVE-2025-40300, CVE-2025-68183, CVE-2025-68284, CVE-2025-68285, CVE-2025-68312, CVE-2025-68771, CVE-2025-68813, CVE-2025-71085, CVE-2025-71089, CVE-2025-71112, CVE-2025-71116, CVE-2025-71120, CVE-2026-22999, CVE-2026-23001, CVE-2022-50329, CVE-2022-50488, CVE-2023-52983)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in the Linux Kernel which is utilized in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise Micro 5.2 and 5.5 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/2026/suse-su-20260496-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20260495-1/

Affected Product	**HPE**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-35998, CVE-2025-30508)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-35998**: Missing protection mechanism for alternate hardware interface in the Intel(R) Quick Assist Technology for some Intel(R) Platforms within Ring 0: Kernel may allow an escalation of privilege. System software adversary with a privileged user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present with special internal knowledge and requires no user interaction. **CVE-2025-30508**: Improper authorization in the Intel(R) Quick Assist Technology for some Intel(R) Platforms within Ring 0: Kernel may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present with special internal knowledge and requires no user interaction. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE ProLiant Compute DL320 Gen12 versions Prior to 1.62_02-06-2026 HPE ProLiant Compute DL340 Gen12 versions Prior to 1.62_02-06-2026 HPE ProLiant Compute DL380a Gen12 versions Prior to 1.62_02-06-2026
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05004en_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.