Advisory Alert

Alert Number: AAA20250527 **Date:** May 27, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in SUSE Linux Kernel. These vulnerabilities could be exploited by malicious users to cause memory leak, memory corruption, system crash. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.6 Public Cloud Module 15-SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-202501707-1/

Affected Product	**Red Hat**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21964, CVE-2024-53104, CVE-2025-21756, CVE-2023-53107)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-21964** - cifs: Fix integer overflow while processing acregmax mount option User-provided mount parameter acregmax of type u32 is intended to have an upper limit, but before it is validated, the value is converted from seconds to jiffies which can lead to an integer overflow. **CVE-2024-53104** - A vulnerability was found in the Linux kernel's USB Video Class driver. A buffer for video frame data is allocated, which does not account for all of the frame formats contained in a video stream, leading to an out-of-bounds write when a stream includes frames with an undefined format. An attacker who is able to influence the format of video streams captured by a system's USB video device could exploit this flaw to alter system memory and potentially escalate their privileges or execute arbitrary code. **CVE-2025-21756** - A flaw was found in the Linux kernel's VMware network driver, where an improperly timed socket unbinding could result in a use-after-free issue. This flaw allows an attacker who can create and destroy arbitrary connections on virtual connections to read or modify system memory, potentially leading to an escalation of privileges or the compromise of sensitive data. **CVE-2023-53107** - A use-after-free vulnerability has been identified within the veth_convert_skb_to_xdp_buff() function of the Linux kernel's veth driver. Successful exploitation of this vulnerability could result in memory corruption, denial of service, and overall system instability. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:8142 • https://access.redhat.com/errata/RHSA-2025:8137 • https://access.redhat.com/errata/RHSA-2025:8134 • https://access.redhat.com/errata/RHSA-2025:8133

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.