Advisory Alert

Alert Number: AAA20250625 **Date:** June 25, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Privilege Escalation Vulnerability
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
Red Hat	**Medium**	Security Update
Ubuntu	**Medium**	Multiple Linux kernel vulnerabilities
F5	**Low**	Memory Leak Vulnerability

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2025-37101)
Description	HPE has released security updates addressing a privilege escalation vulnerability that exist in Their products. **CVE-2025-37101** - A potential security vulnerability has been identified in HPE OneView for VMware vCenter (OV4VC). This vulnerability could be exploited allowing an attacker with read only privilege to cause Vertical Privilege Escalation. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE OneView for VMware vCenter with Operations Manager and Log Insight • All versions prior to v11.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04876en_us&docLocale=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities
Description	SUSE has released security updates addressing multiple linux kernel vulnerabilities that exist in Their products. These vulnerabilities could be exploited by malicious users to cause use-after-free, out-of-bounds access, slab-out-of-bounds. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise High Performance Computing 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502070-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502071-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502072-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502073-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502075-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502076-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502077-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502087-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502090-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502095-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502096-1/

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2022-49328, CVE-2022-49696, CVE-2025-21764)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in Their products. **CVE-2022-49328** - A vulnerability was found in the Linux kernel's mt76 wi-fi driver. A concurrency bug causes the mtxq TX queue to maintain a raw pointer to a wcid structure (mtxq->wcid) that might be freed by the time it is accessed. This issue can lead to a use-after-free scenario, leading to system instability, memory corruption, and potentially arbitrary code execution. **CVE-2022-49696** - A vulnerability was found in the Linux kernel's Transparent Inter-Process Communication (TIPC) subsystem, allowing a use-after-free condition during the cleanup process. This issue arises when the kernel's work queue mechanism does not properly synchronize the destruction of TIPC namespaces with the completion of pending work items. **CVE-2025-21764** - A vulnerability was found in the Linux kernel's IPv6 Neighbor Discovery (NDISC) subsystem, which manages network neighbor information. The issue arises from improper synchronization mechanisms when allocating socket buffers (sk_buff) in the ndisc_alloc_skb() function. Specifically, the function can be called without holding the necessary Read-Copy-Update (RCU) or Routing Netlink (RTNL) locks, leading to a potential use-after-free (UAF) condition. This flaw allows an attacker with local access and low privileges to exploit the race condition, potentially causing system instability or crashes. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:9497 • https://access.redhat.com/errata/RHSA-2025:9498

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Linux kernel vulnerabilities (CVE-2025-40325, CVE-2025-40114, CVE-2025-40014, CVE-2025-39989, CVE-2025-39930, CVE-2025-39778, CVE-2025-39755, CVE-2025-39735, CVE-2025-39728, CVE-2025-39688, CVE-2025-2312, CVE-2025-21943, CVE-2025-21699, CVE-2025-21697, CVE-2025-21694, CVE-2025-21692, CVE-2025-21691, CVE-2025-21690, CVE-2025-21689, CVE-2025-21684)
Description	Ubuntu has released security updates addressing multiple linux kernel vulnerabilities that exist in Their products. These vulnerabilities that could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 20.04, 24.04, 25.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7594-1 • https://ubuntu.com/security/notices/USN-7595-1

Affected Product	**F5**
Severity	**Low**
Affected Vulnerability	Memory Leak Vulnerability (CVE-2019-14834)
Description	F5 has released security updates addressing a memory leak vulnerability that exists in Their products. **CVE-2019-14834** - A vulnerability was found in dnsmasq before version 2.81, where the memory leak allows remote attackers to cause a denial of service (memory consumption) via vectors involving DHCP response creation. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS-A Versions - 1.8.0, 1.5.1 - 1.5.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000152048

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.