Advisory Alert

Alert Number: AAA20250702 **Date:** July 2, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ubuntu	**High**, **Medium**	Multiple Linux kernel vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
F5	**Low**	Unauthorized Access Vulnerability

Description

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Linux kernel vulnerabilities (CVE-2025-37932, CVE-2025-37798, CVE-2024-53197, CVE-2024-50116, CVE-2024-49958, CVE-2024-46787, CVE-2022-49909, CVE-2022-3640, CVE-2021-47576, CVE-2021-47260, CVE-2025-38001, CVE-2025-38000, CVE-2025-37997, CVE-2025-37890, CVE-2024-53051, CVE-2024-50047, CVE-2025-22088)
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 14.04, 16.04, 20.4, 22.04, 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7607-1 • https://ubuntu.com/security/notices/USN-7608-1 • https://ubuntu.com/security/notices/USN-7609-1

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49111, CVE-2022-49114, CVE-2022-49122, CVE-2022-49377, CVE-2022-49407, CVE-2023-1652, CVE-2022-49328, CVE-2022-49395)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 8.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:10174 • https://access.redhat.com/errata/RHSA-2025:10179

Affected Product	**F5**
Severity	**Low**
Affected Vulnerability	Unauthorized Access Vulnerability (CVE-2024-56433)
Description	F5 has released a security update addressing an unauthorized access vulnerability that exists in their products. **CVE-2024-56433** - shadow-utils (aka shadow) 4.4 through 4.17.0 establishes a default /etc/subuid behavior (e.g., uid 100000 through 165535 for the first user account) that can realistically conflict with the uids of users defined on locally administered networks, potentially leading to account takeover, e.g., by leveraging newuidmap for access to an NFS home directory (or same-host resources in the case of remote logins by these local network users). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next SPK Versions - 2.0.0 - 2.0.1, 1.7.0 - 1.9.2 BIG-IP Next CNF Versions - 2.0.0 - 2.0.1, 1.1.0 - 1.4.1 BIG-IP Next for Kubernetes Versions - 2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000152313

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.