Advisory Alert

Alert Number: AAA20251125 **Date:** November 25, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**High**	Security Update
SUSE	**High**	Multiple Vulnerabilities
Dell	**Medium**	Improper Input Validation Vulnerability
Red Hat	**Medium**	Multiple Vulnerabilities
Synology	**Medium**	Local Arbitrary Files write Vulnerability

Description

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2025-40780)
Description	F5 has released security updates addressing a pseudo random number generator (PRNG) weakness in BIND. An attacker can exploit this vulnerability to execute cache poisoning attacks, injecting malicious or spoofed DNS records into the BIG-IP system's resolver functionality. Once poisoned, the BIG-IP system may return incorrect DNS responses to clients, potentially redirecting client traffic to attacker-controlled IPs. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP DNS versions 21.0.0, 17.5.0 - 17.5.1, 17.1.0 - 17.1.3, 16.1.0 - 16.1.6 and 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000157948

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50388, CVE-2022-50432, CVE-2023-53673, CVE-2024-53141, CVE-2025-23145)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3 and 15.4 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3 and 15 SP4 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP3 and 15-SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3 and 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 12 SP5, 15 SP3 and 15 SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3 and 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20254203-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254215-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254213-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254199-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254194-1/

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Improper Input Validation Vulnerability (CVE-2025-33043)
Description	Dell has released security updates addressing an Improper Input Validation Vulnerability that exists in AMI BIOS which affects Dell PowerEdge T40 Mini Tower Server. **CVE-2025-33043** - APTIOV contains a vulnerability in BIOS where an attacker may cause an Improper Input Validation locally. Successful exploitation of this vulnerability can potentially impact of integrity. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerEdge T40 BIOS Versions prior to 1.22.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000395859/dsa-2025-424-security-update-for-dell-poweredge-t40-mini-tower-server-for-an-ami-bios-vulnerability

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50341, CVE-2022-50356, CVE-2022-50386, CVE-2022-50403, CVE-2022-50410, CVE-2023-53232, CVE-2023-53257, CVE-2023-53297, CVE-2023-53354, CVE-2023-53365, CVE-2023-53393, CVE-2024-46679, CVE-2025-38718, CVE-2025-38729, CVE-2025-39697, CVE-2025-39757, CVE-2025-39843, CVE-2025-39883, CVE-2025-39898, CVE-2025-39971, CVE-2025-40047, CVE-2025-40300)
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 the affected system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:22006 • https://access.redhat.com/errata/RHSA-2025:21933 • https://access.redhat.com/errata/RHSA-2025:21926

Affected Product	**Synology**
Severity	**Medium**
Affected Vulnerability	Local Arbitrary Files write Vulnerability (CVE-2025-13593)
Description	Synology has released security updates addressing a Local Arbitrary Files write Vulnerability that exists in ActiveProtect Agent on Windows. **CVE-2025-13593** - Synology ActiveProtect Agent on Windows allows local users to write arbitrary files with restricted content. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ActiveProtect Agent (Windows) versions prior to 1.1.0-0439
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_25_15

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.