TLP: WHITE

Advisory Alert

Alert Number: AAA20260224 **Date:** February 24, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Zyxel	**Critical**	Command Injection Vulnerability
Zyxel	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Synology	**Medium**	DLL Hijacking Vulnerability

Description

Affected Product	**Zyxel**
Severity	**Critical**
Affected Vulnerability	Command Injection Vulnerability (CVE-2025-13942)
Description	Zyxel has released security updates addressing a vulnerability that exists in their Products. **CVE-2025-13942 -** A command injection vulnerability in the UPnP function of certain 4G LTE/5G NR CPE, DSL/Ethernet CPE, Fiber ONTs, and Wireless Extenders firmware versions could allow a remote attacker to execute operating system (OS) commands on an affected device by sending specially crafted UPnP SOAP requests. the attack can be carried out remotely only if both WAN access and the vulnerable UPnP function have been enabled. Zyxel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	LTE3301-PLUS - 1.00(ABQU.8)C0 and earlier NR7101 - 1.00(ABUV.11)C0 and earlier Nebula LTE3301-PLUS - 1.18(ACCA.6)C0 and earlier Nebula NR7101 - 1.16(ACCC.1)C0 and earlier DX4510-B0 - 5.17(ABYL.10)C0 and earlier DX4510-B1 - 5.17(ABYL.10)C0 and earlier EE6510-10 - 5.19(ACJQ.4)C0 and earlier EMG6726-B10A - 5.13(ABNP.8.1)C1 and earlier EX2210-T0 - 5.50(ACDI.2.3)C0 and earlier EX3510-B0 - 5.17(ABUP.15.1)C0 and earlier EX3510-B1 - 5.17(ABUP.15.1)C0 and earlier EX5510-B0 - 5.17(ABQX.11)C0 and earlier EX5512-T0 - 5.70(ACEG.5.3)C0 and earlier EX7710-B0 - 5.18(ACAK.1.5)C0 and earlier VMG4927-B50A - 5.13(ABLY.10.1)C0 and earlier PX3321-T1 - 5.44(ACJB.1.4)C0 and earlier PX3321-T1 - 5.44(ACHK.2)C0 and earlier PX5301-T0 - 5.44(ACKB.0.5)C0 and earlier WX5610-B0 - 5.18(ACGJ.0.4)C0 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-null-pointer-dereference-and-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-security-routers-and-wireless-extenders-02-24-2026

Affected Product	**Zyxel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-1459, CVE-2025-13943, CVE-2025-11848, CVE-2025-11847, CVE-2025-11846, CVE-2025-11845)
Description	Zyxel has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Zyxel 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://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-null-pointer-dereference-and-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-security-routers-and-wireless-extenders-02-24-2026

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-9230, CVE-2025-15467, CVE-2025-55753, CVE-2025-58098, CVE-2025-65082, CVE-2025-66200, CVE-2025-69419, CVE-2025-38129, CVE-2025-38206, CVE-2025-38248, CVE-2025-40064, CVE-2025-68800, CVE-2026-23074, CVE-2025-37861, CVE-2025-38106, CVE-2025-38415, CVE-2025-38730, CVE-2025-39760)
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 for x86_64 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services 1 for RHEL 7 x86_64 Red Hat JBoss Core Services Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:3124 https://access.redhat.com/errata/RHSA-2026:3088 https://access.redhat.com/errata/RHSA-2026:3083 https://access.redhat.com/errata/RHSA-2026:3066 https://access.redhat.com/errata/RHSA-2026:2995 https://access.redhat.com/errata/RHSA-2026:2994

Affected Product	**Synology**
Severity	**Medium**
Affected Vulnerability	DLL Hijacking Vulnerability (CVE-2026-3091)
Description	Synology has released a security update addressing a vulnerability that exists in their products. **CVE-2026-3091** - An uncontrolled search path element vulnerability in Synology Presto Client before 2.1.3-0672 allows local users to read or write arbitrary files during installation by placing a malicious DLL in advance in the same directory as the installer. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Synology Presto Client Versions prior to 2.1.3-0672
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_26_02

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.