Advisory Alert

Alert Number: **AAA20260206** **Date:** **February 6, 2026**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Zyxel	**High**	OS Command Injection Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**Medium**, **Low**	Denial of Service (DoS) Vulnerabilities

Description

Affected Product	**Zyxel**
Severity	**High**
Affected Vulnerability	OS Command Injection Vulnerability (CVE-2025-11730)
Description	Zyxel has released a security update addressing an OS command injection vulnerability that exists in their products. **CVE-2025-11730**: A post-authentication command injection vulnerability in the Dynamic DNS (DDNS) configuration CLI command in certain versions of the ZLD firewall firmware could allow an authenticated attacker with administrator privileges to execute operating system (OS) commands on an affected device by supplying a specially crafted string as an argument to the CLI command. Zyxel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ATP versions ZLD V5.35 to V5.41 USG FLEX versions ZLD V5.35 to V5.41 USG FLEX 50(W)/ USG20(W)-VPN versions ZLD V5.35 to V5.41
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerability-in-the-ddns-configuration-cli-command-of-zld-firewalls-02-05-2026

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-68285, CVE-2025-40248, CVE-2023-53751, CVE-2025-68301, CVE-2022-50865)
Description	Red Hat has released a security update 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 these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 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-2026:2115 https://access.redhat.com/errata/RHSA-2026:2109 https://access.redhat.com/errata/RHSA-2026:2096 https://access.redhat.com/errata/RHSA-2026:1946 https://access.redhat.com/errata/RHSA-2026:2127

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Buffer Overflow, Sensitive Information Leakage, Unauthorized Access, and Cross-Site Request attacks. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	DB2 Recovery Expert for LUW version 5.5 IF 2 AIX version 7.3 VIOS version 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7259901 https://www.ibm.com/support/pages/node/7259886

Affected Product	**F5**
Severity	**Medium**, **Low**
Affected Vulnerability	Denial of Service (DoS) Vulnerabilities (CVE-2025-61725, CVE-2025-58188, CVE-2025-61723, CVE-2021-3737)
Description	F5 has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service (DoS) attacks. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	BIG-IP Next for Kubernetes versions 2.1.0 F5OS-A versions • 1.8.0 to 1.8.3 • 1.5.1 to 1.5.4 F5OS-C versions • 1.8.0 to 1.8.2 • 1.6.0 to 1.6.4 BIG-IP (all modules) versions • 21.0.0 • 17.5.0 to 17.5.1 • 17.1.0 to 17.1.3 • 16.1.0 to 16.1.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000159890 https://my.f5.com/manage/s/article/K000159891 https://my.f5.com/manage/s/article/K000159896 https://my.f5.com/manage/s/article/K000159893

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.