Advisory Alert

Alert Number: **AAA20251118** **Date:** **November 18, 2025**

Document Classification Level **:** Public Circulation Permitted | Public

Information Classification Level **:** TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Zyxel Networks	**High, Medium**	Multiple Vulnerabilities
IBM	**Medium**	Improper Input Validation Vulnerability
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-22916, CVE-2021-41495, CVE-2022-40899, CVE-2023-48795, CVE-2023-5869, CVE-2023-7104, CVE-2024-0985, CVE-2024-24790, CVE-2024-2511, CVE-2024-3219, CVE-2024-35195, CVE-2024-37891, CVE-2024-39689, CVE-2024-47611, CVE-2024-6232, CVE-2024-6345, CVE-2024-6923, CVE-2024-7592, CVE-2025-0938, CVE-2025-21502, CVE-2025-26329, CVE-2025-26483, CVE-2025-31115, CVE-2025-32463, CVE-2025-32745, CVE-2025-32746, CVE-2025-32747, CVE-2025-32749, CVE-2025-32750, CVE-2025-32751, CVE-2025-46371, CVE-2025-46817, CVE-2025-46818, CVE-2025-46819, CVE-2025-49844)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerFlex Software. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerFlex Software Versions prior to 4.8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000391573/dsa-2025-436-security-update-for-dell-powerflex-software-multiple-third-party-component-vulnerabilities

Affected Product	**Zyxel Networks**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-6599, CVE-2025-8693)
Description	Zyxel Networks has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-6599** - The uncontrolled resource consumption vulnerability in the web server of certain 4G LTE/5G NR CPE, DSL/Ethernet CPE, Fiber ONTs, Security Routers, and Wireless Extenders firmware versions could allow an attacker to perform Slowloris-style denial-of-service (DoS) attacks. Such attacks may temporarily block legitimate HTTP requests and partially disrupt access to the web management interface, while other networking services remain unaffected. **CVE-2025-8693** - The post-authentication command injection vulnerability in the "priv" parameter of the CGI program in certain DSL/Ethernet CPE, Fiber ONTs, and Wireless Extenders firmware versions could allow an authenticated attacker to execute operating system (OS) commands on an affected device. It is important to note that WAN access is disabled by default on these devices, and the attack can only succeed if the strong, unique user passwords have been compromised. Zyxel Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products including certain 4G LTE/5G NR CPE, DSL/Ethernet CPE, Fiber ONTs, Security Routers, and Wireless Extenders
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-uncontrolled-resource-consumption-and-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-security-routers-and-wireless-extenders-11-18-2025

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Improper Input Validation Vulnerability
Description	IBM has released security updates addressing an Improper Input Validation Vulnerability that exists in IBM Db2 federated server. A Denial of Service vulnerability in FasterXML Jackson Core, caused by improper input validation by the StreamReadConstraints value field. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause the application to crash. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server versions: • 11.1.0 - 11.1.4.7 • 11.5.0 - 11.5.9 • 12.1.0 - 12.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7250478

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56690, CVE-2025-38351, CVE-2025-38498, CVE-2025-38614, CVE-2025-39697, CVE-2025-39864, CVE-2025-39881, CVE-2025-39903, CVE-2025-39946, CVE-2025-39971, CVE-2025-39982, CVE-2025-39983, CVE-2025-40047)
Description	Red Hat has released security updates addressing a 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 10.0 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x 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 10.0 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 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 9.6 x86_64 Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for x86_64 9 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 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:21563 • https://access.redhat.com/errata/RHSA-2025:21492 • https://access.redhat.com/errata/RHSA-2025:21469 • https://access.redhat.com/errata/RHSA-2025:21463

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.