Advisory Alert

Alert Number: AAA20260128 **Date:** January 28, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	Authentication Bypass Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
OpenSSL	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-24858)
Description	Fortinet has released security updates addressing a vulnerability that exists in their Products. **CVE-2026-24858 -** An Authentication Bypass Using an Alternate Path or Channel vulnerability in FortiOS, FortiManager, FortiAnalyzer may allow an attacker with a FortiCloud account and a registered device to log into other devices registered to other accounts, if FortiCloud SSO authentication is enabled on those devices. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiAnalyzer 7.6 (7.6.0 through 7.6.5) FortiAnalyzer 7.4 (7.4.0 through 7.4.9) FortiAnalyzer 7.2 (7.2.0 through 7.2.11) FortiAnalyzer 7.0 (7.0.0 through 7.0.15) FortiManager 7.6 (7.6.0 through 7.6.5) FortiManager 7.4 (7.4.0 through 7.4.9) FortiManager 7.2 (7.2.0 through 7.2.11) FortiManager 7.0 (7.0.0 through 7.0.15) FortiOS 7.6 (7.6.0 through 7.6.5) FortiOS 7.4 (7.4.0 through 7.4.10) FortiOS 7.2 (7.2.0 through 7.2.12) FortiOS 7.0 (7.0.0 through 7.0.18) FortiProxy 7.6 (7.6.0 through 7.6.4) FortiProxy 7.4 (7.4.0 through 7.4.12) FortiProxy 7.2 (7.2 all versions) FortiProxy 7.0 (7.0 all versions)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-060

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37601, CVE-2025-7783, CVE-2025-25977)
Description	IBM has released security updates addressing Multiple vulnerabilities that exist in their DB2 Products. **CVE-2022-37601 –** A prototype pollution vulnerability in the parseQuery function of the webpack loader-utils JavaScript library allows an attacker to inject or modify properties on object prototypes, potentially leading to altered application behavior, security bypasses, or downstream execution/denial conditions if untrusted input is processed. **CVE-2025-7783 –** A vulnerability in the form-data JavaScript library caused by insufficiently random values in boundary generation can lead to HTTP Parameter Pollution (HPP), allowing crafted multipart requests to manipulate backend input parsing and potentially lead to unauthorized internal requests or logic manipulation. **CVE-2025-25977 –** A prototype pollution issue in the canvg library (via its StyleElement constructor) enables an attacker to inject crafted properties into object prototypes, which can lead to arbitrary code execution in affected environments using vulnerable versions of the library. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM DB2 Data Management Console version 3.1.10, 3.1.11, 3.1.12,.3.1.13, 3.1.13.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7258104

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53539, CVE-2023-53552, CVE-2023-53581, CVE-2025-38051, CVE-2025-39898, CVE-2025-39971, CVE-2025-39993, CVE-2025-40248, CVE-2025-40277, CVE-2023-53034, CVE-2025-37789, CVE-2025-37819, CVE-2025-40258)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel of 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 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:1445 • https://access.redhat.com/errata/RHSA-2026:1444

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37186, CVE-2025-37168, CVE-2025-37169, CVE-2025-37170, CVE-2025-37171, CVE-2025-37172, CVE-2025-37173, CVE-2025-37174, CVE-2025-37175, CVE-2025-37176, CVE-2025-37177, CVE-2025-37178, CVE-2025-37179, CVE-2024-4741, CVE-2026-23592, CVE-2026-23593)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking Fabric Composer 7.x.x: 7.2.3 and below HPE Aruba Networking • Mobility Conductors • Mobility Controllers • WLAN and SD-WAN Gateways Managed by HPE Aruba Networking Central AOS-10.7.x.x: 10.7.2.1 and below AOS-10.4.x.x: 10.4.1.9 and below AOS-8.13.x.x: 8.13.1.0 and below AOS-8.10.x.x: 8.10.0.20 and below HPE Aruba Networking VIA client for Linux version 4.7.5 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04996en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04987en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04994en_us&docLocale=en_US

Affected Product	**OpenSSL**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11187, CVE-2025-15467, CVE-2025-15468, CVE-2025-15469, CVE-2025-66199, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796)
Description	OpenSSL has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. OpenSSL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSSL 3.6.0 – 3.6.0 (patched in 3.6.1) OpenSSL 3.5.0 – 3.5.4 (patched in 3.5.5) OpenSSL 3.4.0 – 3.4.3 (patched in 3.4.4) OpenSSL 3.3.0 – 3.3.5 (patched in 3.3.6) OpenSSL 3.0.0 – 3.0.18 (patched in 3.0.19) OpenSSL 1.1.1 – prior to 1.1.1ze OpenSSL 1.0.2 – prior to 1.0.2zn
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/vulnerabilities/#CVE-2025-11187

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-48924, CVE-2025-41234, CVE-2022-41721, CVE-2025-26791, CVE-2022-37599, CVE-2023-48795, CVE-2022-2596, CVE-2024-51744, CVE-2025-22869, CVE-2025-27789, CVE-2024-30171, CVE-2022-38900, CVE-2022-25858, CVE-2025-57810, CVE-2022-25883, CVE-2022-25881, CVE-2025-41249, CVE-2024-38820, CVE-2024-48948, CVE-2024-38816, CVE-2024-4067, CVE-2023-26136, CVE-2024-4068, CVE-2025-5889, CVE-2024-30172, CVE-2024-45338, CVE-2024-38828, CVE-2024-48949)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM DB2 Data Management Console version 3.1.10, 3.1.11, 3.1.12,.3.1.13, 3.1.13.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7258104

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.