Advisory Alert

Alert Number: AAA20250818 **Date:** August 18, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Ivanti	**High**	Multiple Vulnerabilities
Red Hat	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Fortinet	Medium	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-6547, CVE-2025-6545, CVE-2025-7783)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM includes components. **CVE-2025-6547** - Improper Input Validation vulnerability in pbkdf2 allows Signature Spoofing by Improper Validation.This issue affects pbkdf2: <=3.1.2. **CVE-2025-6545** - Improper Input Validation vulnerability in pbkdf2 allows Signature Spoofing by Improper Validation. This vulnerability is associated with program files lib/to-buffer.Js. This issue affects pbkdf2: from 3.0.10 through 3.1.2. **CVE-2025-7783** - Use of Insufficiently Random Values vulnerability in form-data allows HTTP Parameter Pollution (HPP). This vulnerability is associated with program files lib/form_data.Js. This issue affects form-data: < 2.5.4, 3.0.0 - 3.0.3, 4.0.0 - 4.0.3. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Log Source Management App Versions - 1.0.0 - 7.0.11 IBM QRadar Data Synchronization App Versions - 1.0.0 - 3.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7242291 • https://www.ibm.com/support/pages/node/7242292

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-8296, CVE-2025-8297)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-8296** - SQL injection in Ivanti Avalanche before version 6.4.8.8008 allows a remote authenticated attacker with admin privileges to execute arbitrary SQL queries. In certain conditions, this can also lead to remote code execution. **CVE-2025-8297** - Incomplete restriction of configuration in Ivanti Avalanche before version 6.4.8.8008 allows a remote authenticated attacker with admin privileges to achieve remote code execution. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Avalanche Versions - 6.4.6 and prior to 6.4.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-CVE-2025-8296-CVE-2025-8297?language=en_US

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22097, CVE-2025-37914, CVE-2025-38250, CVE-2025-38380, CVE-2024-28956, CVE-2025-21867, CVE-2025-38084, CVE-2025-38085, CVE-2025-38124, CVE-2025-38159, CVE-2025-38471)
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 8 aarch64, 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 Enterprise Linux Server - AUS 9.6 x86_64, for Real Time 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le, 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 8 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, 8 aarch64, 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, 8 s390x, 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le, 9 ppc64le Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64, 8 x86_64, 9 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 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-2025:13960 • https://access.redhat.com/errata/RHSA-2025:13961 • https://access.redhat.com/errata/RHSA-2025:13962

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-7339, CVE-2025-30360, CVE-2025-30359, CVE-2025-32997, CVE-2025-32996, CVE-2025-27789, CVE-2025-5889, CVE-2025-26791, CVE-2024-11831, CVE-2025-48050, CVE-2025-22150, CVE-2025-23085)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM includes components. These vulnerabilities could be exploited by malicious users to cause cross-site scripting, denial of service, memory leak. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Log Source Management App Versions - 1.0.0 - 7.0.11 IBM QRadar Data Synchronization App Versions - 1.0.0 - 3.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7242291 • https://www.ibm.com/support/pages/node/7242292

Affected Product	**Fortinet**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-40588, CVE-2024-52964)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-40588** - Multiple relative path traversal vulnerabilities [CWE-23] in FortiMail, FortiVoice, FortiRecorder, FortiCamera & FortiNDR may allow a privileged attacker to read files from the underlying filesystem via crafted CLI requests. **CVE-2024-52964** - An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability [CWE-22] in FortiManager & FortiManager Cloud may allow an authenticated remote attacker to overwrite arbitrary files via FGFM crafted requests. Fortinet 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.fortiguard.com/psirt/FG-IR-24-309 • https://www.fortiguard.com/psirt/FG-IR-24-473

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.