Advisory Alert

Alert Number: AAA20260731 **Date:** July 31, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Apache Tomcat	**Low**	Uncontrolled Resource Consumption Vulnerability

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-4800, CVE-2025-7783)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-4800:** When an application passes untrusted input as options.imports key names, an attacker can inject default-parameter expressions that execute arbitrary code at template compilation time. Additionally, _.template uses assignInWith to merge imports, which enumerates inherited properties via for..in. If Object.prototype has been polluted by any other vector, the polluted keys are copied into the imports object and passed to Function(). **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. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Data Synchronization App versions 1.0.0 to 3.3.0 IBM QRadar Pulse App 1.0.0 to 2.2.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7281949 https://www.ibm.com/support/pages/node/7281950

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-13465, CVE-2026-2950, CVE-2026-41907, CVE-2026-41988, CVE-2026-42338, CVE-2026-5038, CVE-2026-5079, CVE-2026-13149, CVE-2025-15284, CVE-2026-33750, CVE-2026-29786, CVE-2026-31802, CVE-2026-4867, CVE-2026-8723, CVE-2026-5758, CVE-2026-53550, CVE-2026-12143, CVE-2026-23950, CVE-2026-24842, CVE-2026-26960, CVE-2026-53655, CVE-2026-59869, CVE-2025-27789, CVE-2025-47935, CVE-2025-47944, CVE-2024-12905, CVE-2025-48997, CVE-2025-5889, CVE-2025-7338, CVE-2025-59343, CVE-2025-12758, CVE-2025-64718, CVE-2026-2391, CVE-2026-26996, CVE-2026-27903, CVE-2026-27904, CVE-2026-3449, CVE-2026-2359, CVE-2026-3304, CVE-2026-3520, CVE-2026-12590, CVE-2025-56200, CVE-2026-59871, CVE-2026-59873, CVE-2026-59874, CVE-2026-59875, CVE-2025-48387, CVE-2026-23745)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM QRadar Data Synchronization App versions 1.0.0 to 3.3.0 IBM QRadar Pulse App 1.0.0 to 2.2.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7281949 https://www.ibm.com/support/pages/node/7281950

Vendor	**Apache Tomcat**
Severity	**Low**
Affected Vulnerability	Uncontrolled Resource Consumption Vulnerability (CVE-2026-66299)
Description	Apache Tomcat has released security updates addressing a vulnerability that exists in their products. **CVE-2026-66299:** The WebSocket chat example provided an unbounded buffer for undelivered messages. A maliciously slow client could cause the buffer to grow continuously, eventually leading to an memory exhaustion and failure of the Tomcat process. Apache Tomcat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache Tomcat versions: • 11.0.0-M20 to 11.0.24 • 10.1.24 to 10.1.57 • 9.0.89 to 9.0.120
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tomcat.apache.org/security-11.html https://tomcat.apache.org/security-10.html https://tomcat.apache.org/security-9.html

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.