



Advisory Alert

Alert Number: AAA20251128 Date: November 28, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	Critical	Use of Insufficiently Random Values Vulnerability
SUSE	High	Multiple Vulnerabilities
IBM	High, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	IBM
Severity	Critical
Affected Vulnerability	Use of Insufficiently Random Values Vulnerability (CVE-2025-7783)
Description	IBM has released security updates addressing a Use of Insufficiently Random Values Vulnerability that exists in a third party component which affects IBM QRadar Deployment Intelligence App. 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 Deployment Intelligence App versions 1.0.0 - 3.0.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7252903

Affected Product	SUSE
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53673, CVE-2024-53141, CVE-2025-23145, CVE-2025-38500, CVE-2025-38616)
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4, 15.5 and 15.6 SUSE Linux Enterprise High Performance Computing 15 SP4 and 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5 and 15-SP6 SUSE Linux Enterprise Micro 5.3, 5.4 and 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 and 15 SP6 SUSE Linux Enterprise Server 15 SP4, 15 SP5 and 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP5 and 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none">https://www.suse.com/support/update/announcement/2025/suse-su-20254283-1/https://www.suse.com/support/update/announcement/2025/suse-su-20254282-1/https://www.suse.com/support/update/announcement/2025/suse-su-20254281-1/https://www.suse.com/support/update/announcement/2025/suse-su-20254275-1/https://www.suse.com/support/update/announcement/2025/suse-su-20254269-1/

Affected Product	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-25031, CVE-2025-47279, CVE-2025-48924, CVE-2025-54121, CVE-2025-58057, CVE-2025-58369, CVE-2025-58754, CVE-2025-59822, CVE-2025-7339)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar components. These vulnerabilities could be exploited by malicious users to cause denial of service, memory leak, security restrictions bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar EDR versions 3.12 - 3.12.20 IBM QRadar Deployment Intelligence App versions 1.0.0 - 3.0.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none">https://www.ibm.com/support/pages/node/7252908https://www.ibm.com/support/pages/node/7252903

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.