Advisory Alert

Alert Number: AAA20250519 **Date:** May 19, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**Medium**	Linux kernel vulnerabilities
WatchGuard	**Medium**	Multiple Cross Site Scripting Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-36182, CVE-2020-36186, CVE-2020-11620, CVE-2017-7525, CVE-2018-12022, CVE-2020-11619, CVE-2020-9546, CVE-2020-10673, CVE-2020-8840, CVE-2020-11112, CVE-2020-9548, CVE-2020-14062, CVE-2020-36181, CVE-2020-36185, CVE-2020-10969, CVE-2020-24616, CVE-2019-14893, CVE-2017-17485, CVE-2020-9547, CVE-2020-11111, CVE-2020-10672, CVE-2020-14195, CVE-2019-16943, CVE-2020-36180, CVE-2020-36184, CVE-2019-12384, CVE-2018-14719, CVE-2021-20190, CVE-2020-36188, CVE-2020-14060, CVE-2020-24750, CVE-2020-36189, CVE-2020-36183, CVE-2020-36187, CVE-2020-36179, CVE-2020-10968, CVE-2017-15095, CVE-2018-14721, CVE-2019-17531, CVE-2020-14061, CVE-2018-14718, CVE-2019-14892, CVE-2019-16942, CVE-2020-11113, CVE-2019-14379, CVE-2021-20086, CVE-2024-40464, CVE-2024-45337, CVE-2024-38821, CVE-2019-10744)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to cause Improper Certificate Validation, authorization bypass, Allocation of Resources Without Limits or Throttling, Deserialization of Untrusted Data. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Copy Data Management - Versions 2.2.0.0 - 2.2.25.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7232411 • https://www.ibm.com/support/pages/node/7232415 • https://www.ibm.com/support/pages/node/7232417

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47671, CVE-2022-49741, CVE-2024-46784, CVE-2025-21726, CVE-2025-21785, CVE-2025-21791, CVE-2025-21812, CVE-2025-21886, CVE-2025-22004, CVE-2025-22020, CVE-2025-22029, CVE-2025-22045, CVE-2025-22055, CVE-2025-22097, CVE-2020-36789, CVE-2021-47163, CVE-2021-47668, CVE-2021-47669, CVE-2021-47670, CVE-2022-49111, CVE-2023-0179, CVE-2023-53026, CVE-2023-53033, CVE-2024-56642, CVE-2024-56661)
Description	SUSE has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to cause out-of-bounds write, integer overflow, use after free and double free. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.2, 5.3, 5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20251573-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251574-1/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53141, CVE-2025-21756, CVE-2025-21966, CVE-2025-37749)
Description	Red Hat has released security updates addressing multiple vulnerabilities in their products. these vulnerabilities could be exploited by malicious users to cause memory corruption, missing range check, Keep the binding until socket destruction. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:7896 • https://access.redhat.com/errata/RHSA-2025:7902 • https://access.redhat.com/errata/RHSA-2025:7903

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21587, CVE-2025-4447, CVE-2023-52492, CVE-2024-24857, CVE-2022-48912, CVE-2024-27017, CVE-2022-48773, CVE-2024-27043, CVE-2024-26929, CVE-2024-41042, CVE-2022-42004, CVE-2019-12814, CVE-2019-17267, CVE-2018-14720, CVE-2018-12023, CVE-2019-14540, CVE-2018-5968, CVE-2019-20330, CVE-2018-7489, CVE-2018-19362, CVE-2019-10202, CVE-2020-25649, CVE-2020-36518, CVE-2019-12086, CVE-2019-14439, CVE-2018-11307, CVE-2018-19361, CVE-2022-42003, CVE-2019-16335, CVE-2018-19360, CVE-2020-10650, CVE-2020-11022, CVE-2015-9251, CVE-2019-11358, CVE-2020-11023, CVE-2020-23064, CVE-2022-31129, CVE-2022-24785, CVE-2019-10172, CVE-2025-22869, CVE-2022-31836, CVE-2019-16354, CVE-2019-16355, CVE-2024-40465, CVE-2022-31259, CVE-2021-22112, CVE-2016-5007, CVE-2022-22978, CVE-2016-9879, CVE-2019-1010266, CVE-2020-28500, CVE-2018-16487, CVE-2018-3721, CVE-2020-8203, CVE-2021-23337)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. these vulnerabilities could be exploited by malicious users to cause Improper Access Control, Buffer Overflow, NULL Pointer Dereference, Use After Free. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server - Versions 8.5, 9.0 IBM Storage Copy Data Management - Versions 2.2.0.0 - 2.2.25.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7233442 • https://www.ibm.com/support/pages/node/7232419 • https://www.ibm.com/support/pages/node/7232415 • https://www.ibm.com/support/pages/node/7232418 • https://www.ibm.com/support/pages/node/7232417 • https://www.ibm.com/support/pages/node/7232411

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Linux kernel vulnerabilities (CVE-2025-21971, CVE-2025-21951, CVE-2025-21950, CVE-2025-21948, CVE-2025-21943, CVE-2025-21935, CVE-2025-21934, CVE-2025-21928, CVE-2025-21926, CVE-2025-21925)
Description	Ubuntu has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Access bypass, Denial of Service, Cross Site Scripting. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04, 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7510-1

Affected Product	**WatchGuard**
Severity	**Medium**
Affected Vulnerability	Multiple Cross Site Scripting Vulnerabilities (CVE-2025-4804, CVE-2025-4805)
Description	WatchGuard has released security updates addressing multiple vulnerabilities in their products. **CVE-2025-4804 -** A stored cross-site scripting (XSS) vulnerability exists in the management interface of WatchGuard Firebox appliances via the Hotspit configuration. An authenticated remote attacker with administrator privileges could exploit this vulnerability to execute arbitrary JavaScript code in the Firebox management interface of another management user. **CVE-2025-4805 -** A stored cross-site scripting (XSS) vulnerability exists in the management interface of WatchGuard Firebox appliances via the Access Portal configuration. An authenticated remote attacker with administrator privileges could exploit this vulnerability to execute arbitrary JavaScript code in the Firebox management interface of another management user. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Fireware OS: from 12.0 up to and including 12.11.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00006 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00007

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.