# Advisory Alert

**Alert Number:** AAA20260327 **Date:** March 27, 2026

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **IBM** | **Critical** | Multiple Vulnerabilities |
| **SUSE** | **High** | Multiple Vulnerabilities |
| **IBM** | **High, Medium** | Multiple Vulnerabilities |
| **Hitachi** | **High, Medium** | Multiple Vulnerabilities |
| **WatchGaurd** | **Medium** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-1188, CVE-2022-46337, CVE-2025-48913) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products.<br><br>**CVE-2026-1188:** In the Eclipse OMR port library component, an API function to return the textual names of all supported processor features was not accounting for the separator inserted between processor features. If the output buffer supplied to this function was incorrectly sized, failing to account for the separator when determining when a write to the buffer was safe could lead to a buffer overflow.<br><br>**CVE-2022-46337:** A vulnerability in LDAP-authenticated Derby installations allows a clearly devised username to bypass authentication checks. This could also allow the attacker to execute malware which was visible to and executable by the account which booted the Derby server. In LDAP-protected databases which weren't also protected by SQL GRANT/REVOKE authorization, this vulnerability could also let an attacker view and corrupt sensitive data and run sensitive database functions and procedures.<br><br>**CVE-2025-48913:** If untrusted users are allowed to configure JMS for Apache CXF, previously they could use RMI or LDAP URLs, potentially leading to code execution capabilities. This interface is now restricted to reject those protocols, removing this possibility.<br><br>IBM advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | QRadar – Versions 7.5.0 - 7.5.0 UP14 IF05<br>WebSphere Extreme Scale – Versions 8.6.1.0 - 8.6.1.6 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7267689<br>• https://www.ibm.com/support/pages/node/7266711 |

| | |
|---|---|
| Affected Product | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | SUSE 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 the affected systems.<br><br>SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | openSUSE Leap 15.5<br>openSUSE Leap 15.6<br>SUSE Linux Enterprise High Performance Computing 15 SP5<br>SUSE Linux Enterprise High Performance Computing 12 SP5<br>SUSE Linux Enterprise Live Patching 15-SP5<br>SUSE Linux Enterprise Live Patching 12-SP5<br>SUSE Linux Enterprise Live Patching 15-SP6<br>SUSE Linux Enterprise Live Patching 15-SP7<br>SUSE Linux Enterprise Micro 5.5<br>SUSE Linux Enterprise Real Time 15 SP5<br>SUSE Linux Enterprise Real Time 15 SP6<br>SUSE Linux Enterprise Real Time 15 SP7<br>SUSE Linux Enterprise Server 15 SP5<br>SUSE Linux Enterprise Server 15 SP6<br>SUSE Linux Enterprise Server 15 SP7<br>SUSE Linux Enterprise Server 12 SP5<br>SUSE Linux Enterprise Server 12 SP5 LTSS<br>SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security<br>SUSE Linux Enterprise Server for SAP Applications 15 SP5<br>SUSE Linux Enterprise Server for SAP Applications 15 SP6<br>SUSE Linux Enterprise Server for SAP Applications 15 SP7<br>SUSE Linux Enterprise Server for SAP Applications 12 SP5<br>SUSE Linux Enterprise Desktop 15 SP7<br>SUSE Linux Enterprise High Availability Extension 15 SP7<br>SUSE Linux Enterprise Workstation Extension 15 SP7<br>Basesystem Module 15-SP7<br>Development Tools Module 15-SP7<br>Legacy Module 15-SP7<br>Public Cloud Module 15-SP7 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.suse.com/support/update/ |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High, Medium** |
| Affected Vulnerability | Multiple Vulnerability (CVE-2026-21945, CVE-2026-21932, CVE-2026-21933, CVE-2026-21925, CVE-2022-50673, CVE-2025-38403, CVE-2025-40135, CVE-2025-40158, CVE-2025-40170, CVE-2025-40269, CVE-2025-68349, CVE-2026-22998, CVE-2025-5372, CVE-2025-66471, CVE-2025-66418, CVE-2026-21441, CVE-2025-9086, CVE-2025-53905, CVE-2025-53906, CVE-2025-14104, CVE-2022-50865, CVE-2024-26766, CVE-2025-38022, CVE-2025-38024, CVE-2025-38415, CVE-2025-38459, CVE-2025-39760, CVE-2025-40258, CVE-2025-40271, CVE-2025-40322, CVE-2023-53552, CVE-2025-38051, CVE-2025-39933, CVE-2025-40096, CVE-2025-68301, CVE-2025-6176, CVE-2025-8916, CVE-2025-14242, CVE-2025-12084, CVE-2025-64775, CVE-2025-66675, CVE-2025-15366, CVE-2025-15367, CVE-2026-0865, CVE-2026-1299, CVE-2025-27533, CVE-2025-4897, CVE-2025-66453, CVE-2025-48924, CVE-2025-23184, CVE-2025-58457, CVE-2023-44483.) |
| 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.<br><br>IBM advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | QRadar – Versions 7.5.0 - 7.5.0 UP14 IF05<br>WebSphere Extreme Scale – Versions 8.6.1.0 - 8.6.1.6 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7267689<br>• https://www.ibm.com/support/pages/node/7266711 |

| | |
|---|---|
| Affected Product | **Hitachi** |
| Severity | **High, Medium** |
| Affected Vulnerability | Multiple Vulnerability (CVE-2026-20846, CVE-2026-21222, CVE-2026-21231, CVE-2026-21234, CVE-2026-21235, CVE-2026-21236, CVE-2026-21237, CVE-2026-21238, CVE-2026-21239, CVE-2026-21240, CVE-2026-21242, CVE-2026-21244, CVE-2026-21246, CVE-2026-21247, CVE-2026-21248, CVE-2026-21249, CVE-2026-21253, CVE-2026-21255, CVE-2026-21508, CVE-2026-21510, CVE-2026-21513, CVE-2026-21519, CVE-2026-21525, CVE-2026-21533, CVE-2025-2902, CVE-2025-2514, CVE-2025-1978, CVE-2025-0824, and CVE-2025-9661) |
| Description | Hitachi has released security updates addressing multiple vulnerabilities that exist in their Hitachi Virtual Storage product. These vulnerabilities could be exploited by malicious users to compromise the affected systems.<br><br>Hitachi advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Hitachi Virtual Storage One Block Series<br>• 23, 24, 26, 28<br><br>Hitachi Virtual Storage G Series<br>• G130, G150, G350, G370, G700, G900<br><br>Hitachi Virtual Storage F Series<br>• F350, F370, F700, F900<br><br>Hitachi Virtual Storage E Series<br>• E390, E590, E790, E990, E1090<br>• E390H, E590H, E790H, E1090H<br><br>Hitachi Virtual Storage 5000 Series<br>• 5100, 5500, 5100H, 5500H<br>• 5200, 5600, 5200H, 5600H<br><br>Hitachi Virtual Storage VX Series<br>• VX8 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_309.html<br>• https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_308.html<br>• https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_307.html<br>• https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_306.html<br>• https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_305.html<br>• https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/02.html |

| | |
|---|---|
| Affected Product | **WatchGaurd** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-4315, CVE-2026-4266) |
| Description | WatchGaurd has released security updates addressing multiple vulnerabilities that exist in their Firebox products.<br><br>**CVE-2026-4315:** A Cross-Site Request Forgery (CSRF) vulnerability in the WatchGuard Fireware OS WebUI could allow a remote attacker to trigger a denial-of-service (DoS) condition in the Fireware Web UI by convincing an authenticated administrator into visiting a malicious web page.<br><br>**CVE-2026-4266:** An Insecure Deserialization vulnerability in WatchGuard Fireware OS allows an attacker that has obtained write access to the local filesystem through another vulnerability to execute arbitrary code in the context of the portald user.<br><br>WatchGaurd advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Fireware OS 12.5.x (Prior to 12.5.18)<br>• T15, T35<br>Fireware OS 12.x (Prior to 2026.2)<br>• T20, T25, T40, T45, T55, T70, T80, T85, M270, M290, M370, M390, M470, M570, M590, M670, M690, M440, M4600, M4800, M5600, M5800, Firebox Cloud, Firebox NV5, FireboxV<br>Fireware OS 2025.1.x (Prior to 12.12)<br>• T115-W, T125, T125-W, T145, T145-W, T185, M295, M395, M495, M595, M695 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00006<br>• https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00007 |

**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.**