# Advisory Alert

**Alert Number:** **AAA20250911** **Date:** **September 11, 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 |
| **Dell** | **High** | Multiple Vulnerabilities |
| **Red Hat** | **High** | Multiple Vulnerabilities |
| **SUSE** | **High** | Multiple Vulnerabilities |
| **Cisco** | **High**, **Medium** | Multiple Vulnerabilities |
| **IBM** | **High**, **Medium** | Multiple Vulnerabilities |
| **NetApp** | **High**, **Medium**, **Low** | Multiple Vulnerabilities |
| **Palo Alto Networks** | **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 a security update addressing a Use of Insufficiently Random Values vulnerability that exists in IBM QRadar investigation assistant.<br>**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.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | IBM QRadar Investigation Assistant - 1.0.0 - 1.1.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7244494 |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerProtect Data Manager. These vulnerabilities could be exploited by malicious users to compromise the affected system.<br>Dell advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Dell PowerProtect Data Manager - Versions prior to 19.21 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000367456/dsa-2025-326-security-update-for-dell-powerprotect-data-manager-multiple-security-vulnerabilities |

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-38352, CVE-2025-22097, CVE-2025-38332, CVE-2025-38352, CVE-2025-38449, CVE-2022-50000, CVE-2023-2513, CVE-2025-21759, CVE-2025-38085, CVE-2025-38159, CVE-2025-38464, CVE-2022-50211, CVE-2025-22058, CVE-2024-13009) |
| 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 affected systems.<br>Red Hat 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://access.redhat.com/errata/RHSA-2025:15662<br>• https://access.redhat.com/errata/RHSA-2025:15661<br>• https://access.redhat.com/errata/RHSA-2025:15660<br>• https://access.redhat.com/errata/RHSA-2025:15656<br>• https://access.redhat.com/errata/RHSA-2025:15649<br>• https://access.redhat.com/errata/RHSA-2025:15648<br>• https://access.redhat.com/errata/RHSA-2025:15647<br>• https://access.redhat.com/errata/RHSA-2025:15643<br>• https://access.redhat.com/errata/RHSA-2025:15647 |

| | |
|---|---|
| Affected Product | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-37890, CVE-2025-38000, CVE-2025-38001, CVE-2025-38212, CVE-2025-21999, CVE-2022-49053, CVE-2024-47674, CVE-2024-47706, CVE-2024-49867) |
| 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 systems.<br>SUSE advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | • openSUSE Leap 15.3<br>• SUSE Linux Enterprise High Performance Computing 15 SP3<br>• SUSE Linux Enterprise Live Patching 15-SP3<br>• SUSE Linux Enterprise Micro 5.1<br>• SUSE Linux Enterprise Micro 5.2<br>• SUSE Linux Enterprise Server 15 SP3<br>• SUSE Linux Enterprise Server for SAP Applications 15 SP3<br>• SUSE Linux Enterprise High Performance Computing 12 SP5<br>• SUSE Linux Enterprise Live Patching 12-SP5<br>• SUSE Linux Enterprise Server 12 SP5<br>• SUSE Linux Enterprise Server for SAP Applications 12 SP5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.suse.com/support/update/announcement/2025/suse-su-202503154-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503153-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503149-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503148-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503133-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503143-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503138-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503135-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503130-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503129-1/ |

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-20340, CVE-2025-20248, CVE-2025-20159) |
| Description | Cisco has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2025-20340** - A vulnerability in the Address Resolution Protocol (ARP) implementation of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to trigger a broadcast storm, leading to a denial of service (DoS) condition on an affected device.<br>**CVE-2025-20248** - A vulnerability in the installation process of Cisco IOS XR Software could allow an authenticated, local attacker to bypass Cisco IOS XR Software image signature verification and load unsigned software on an affected device. To exploit this vulnerability, the attacker must have root-system privileges on the affected device.<br>**CVE-2025-20159** - A vulnerability in the management interface access control list (ACL) processing feature in Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass configured ACLs for the SSH, NetConf, and gRPC features.<br>Cisco 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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xrsig-UY4zRUCG<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-arp-storm-EjUU55yM<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-acl-packetio-Swjhhbtz |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-26791, CVE-2025-48976, CVE-2020-36732) |
| Description | IBM has released security updates addressing multiple vulnerabilities in their products.<br>**CVE-2025-26791** - DOMPurify before 3.2.4 has an incorrect template literal regular expression, sometimes leading to mutation cross-site scripting (mXSS).<br>**CVE-2025-48976** - Allocation of resources for multipart headers with insufficient limits enabled a DoS vulnerability in Apache Commons FileUpload. This issue affects Apache Commons FileUpload: from 1.0 before 1.6; from 2.0.0-M1 before 2.0.0-M4.<br>**CVE-2020-36732** - The crypto-js package before 3.2.1 for Node.js generates random numbers by concatenating the string "0." with an integer, which makes the output more predictable than necessary.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | • IBM QRadar Investigation Assistant - 1.0.0 - 1.1.0<br>• IBM WebSphere Application Server - 8.5, 9.0<br>• IBM WebSphere Application Server Liberty - 17.0.0.3 - 25.0.0.9<br>• IBM Db2 v10.5, v11.1, v11.5, v12.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7242088<br>• https://www.ibm.com/support/pages/node/7244494<br>• https://www.ibm.com/support/pages/node/7244513<br>• https://www.ibm.com/support/pages/node/7244573 |

| Affected Product | **NetApp** |
|---|---|
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | NetApp 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.<br>NetApp 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://security.netapp.com/advisory/ |

| Affected Product | **Palo Alto Networks** |
|---|---|
| Severity | **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-4235, CVE-2025-4234) |
| Description | Palo Alto Networks has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2025-4235** - An information exposure vulnerability in the Palo Alto Networks User-ID Credential Agent (Windows-based) can expose the service account password under specific non-default configurations. This allows an unprivileged Domain User to escalate privileges by exploiting the account’s permissions.<br>**CVE-2025-4234** - A problem with the Palo Alto Networks Cortex XDR Microsoft 365 Defender Pack can result in exposure of user credentials in application logs. Normally, these application logs are only viewable by local users and are included when generating logs for troubleshooting purposes. This means that these credentials are exposed to recipients of the application logs.<br>Palo Alto Networks advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | User-ID Credential Agent - versions 11.0.2-133 - 11.0.3 on Windows<br>Cortex XDR Microsoft 365 Defender Pack - Versions prior to 4.6.5 on Windows |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://security.paloaltonetworks.com/CVE-2025-4234<br>• https://security.paloaltonetworks.com/CVE-2025-4235 |

**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.**