# Advisory Alert

**Alert Number:** AAA20251016 **Date:** October 16, 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 Linux Kernel Vulnerabilities |
| **Dell** | **High**, **Medium** | Multiple Vulnerabilities |
| **Cisco** | **High**, **Medium** | Multiple Vulnerabilities |
| **IBM** | **High**, **Medium**, **Low** | Multiple Vulnerabilities |
| **F5** | **High**, **Medium**, **Low** | Multiple Vulnerabilities |
| **Red Hat** | **Medium** | 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 their products.<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 Security QRadar EDR - Versions 3.12 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7247975 |

| | |
|---|---|
| Affected Product | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Linux Kernel Vulnerabilities |
| Description | SUSE has released security updates addressing multiple linux kernel vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system.<br>SUSE advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | OpenSUSE Leap 15.6<br>Legacy Module 15-SP6, 15-SP7<br>Basesystem Module 15-SP6, 15-SP7<br>Confidential Computing Module 15-SP6<br>Development Tools Module 15-SP6, 15-SP7<br>SUSE Linux Enterprise Desktop 15 SP6, 15 SP7<br>SUSE Linux Enterprise High Availability Extension 15 SP6<br>SUSE Linux Enterprise High Availability Extension 15 SP7<br>SUSE Linux Enterprise Live Patching 15-SP6, 15-SP7<br>SUSE Linux Enterprise Real Time 15 SP6, 15 SP7<br>SUSE Linux Enterprise Server 15 SP6, 15 SP7<br>SUSE Linux Enterprise Server for SAP Applications 15 SP6<br>SUSE Linux Enterprise Server for SAP Applications 15 SP7<br>SUSE Linux Enterprise Workstation Extension 15 SP6, 15 SP7 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.suse.com/support/update/announcement/2025/suse-su-202503600-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503601-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503602-1/ |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-20037, CVE-2025-20067, CVE-2025-22392, CVE-2025-6395, CVE-2025-32988, CVE-2025-32989, CVE-2025-32990, CVE-2025-7425, CVE-2023-40403, CVE-2025-7424, CVE-2025-0033) |
| Description | Dell 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>Dell advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | PowerEdge T40 BIOS Versions prior to 1.21.0<br>Dell Networking OS10 Versions prior to 10.6.0.6<br>PowerEdge R6715 BIOS Versions prior to 1.3.3<br>PowerEdge R7715 BIOS Versions prior to 1.3.3<br>PowerEdge R6725 BIOS Versions prior to 1.3.3<br>PowerEdge R7725 BIOS Versions prior to 1.3.3<br>PowerEdge R7725xd BIOS Versions prior to 1.3.3<br>PowerEdge M7725 BIOS Versions prior to 1.3.4<br>PowerEdge XE7745 BIOS Versions prior to 1.3.4<br>PowerEdge R6615 BIOS Versions prior to 1.14.1<br>PowerEdge R7615 BIOS Versions prior to 1.14.1<br>PowerEdge R6625 BIOS Versions prior to 1.14.1<br>PowerEdge R7625 BIOS Versions prior to 1.14.1<br>PowerEdge C6615 BIOS Versions prior to 1.9.1<br>PowerEdge XE9685L BIOS Versions prior to 1.1.5<br>PowerEdge R6515 BIOS Versions prior to 2.21.1<br>PowerEdge R6525 BIOS Versions prior to 2.21.1<br>PowerEdge R7515 BIOS Versions prior to 2.21.1<br>PowerEdge R7525 BIOS Versions prior to 2.21.1<br>PowerEdge C6525 BIOS Versions prior to 2.21.1<br>PowerEdge XE8545 BIOS Versions prior to v2.19.1<br>Dell EMC XC Core XC7525 BIOS Versions prior to 2.21.1<br>Dell XC Core XC7625 BIOS Versions prior to 1.14.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.dell.com/support/kbdoc/en-us/000379613/dsa-2025-371-security-update-for-dell-poweredge-t40-mini-tower-server-for-2025-3-ipu-intel-chipset-firmware-vulnerabilities<br>• https://www.dell.com/support/kbdoc/en-us/000379661/dsa-2025-352-security-update-for-dell-amd-based-poweredge-server-vulnerabilities<br>• https://www.dell.com/support/kbdoc/en-us/000379666/dsa-2025-394-security-update-for-dell-networking-os10-vulnerabilities |

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-20313, CVE-2025-20314, CVE-2025-20350, CVE-2025-20351, CVE-2025-20329, CVE-2025-20359, CVE-2025-20360) |
| Description | Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause cross-site scripting, privilege escalation, information disclosure, denial of service.<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-secboot-UqFD8AvC<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-dos-FPyjLV7A<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-inf-disc-qGgsbxAm<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-mime-vulns-tTL8PgVH |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-5889, CVE-2025-48387, CVE-2025-50181, CVE-2025-50182, CVE-2024-47081, CVE-2020-10735, CVE-2025-22868, CVE-2025-53864, CVE-2025-47278, CVE-2025-47273, CVE-2025-46548, CVE-2019-9674, CVE-2022-38750, CVE-2023-44389, CVE-2022-38751, CVE-2023-32082, CVE-2022-31628, CVE-2023-36479, CVE-2022-38749, CVE-2018-8740, CVE-2025-7338, CVE-2025-27818, CVE-2025-27817, CVE-2025-48997) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Information Disclosure, Execute Unauthorized Code or Commands, Escalation of privilege.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | IBM Security QRadar EDR Versions - 3.12 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7247975 |

| | |
|---|---|
| Affected Product | **F5** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-61974, CVE-2025-53474, CVE-2025-58153, CVE-2025-61958, CVE-2025-20093) |
| Description | F5 has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause privilege escalation, privilege escalation and denial-of-service.<br>F5 advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | F5 Silverline (all services)<br>BIG-IP Next for Kubernetes - 2.0.0 - 2.1.0<br>F5OS-A Versions - 1.8.0 - 1.8.3, 1.5.1 - 1.5.4<br>BIG-IP Next SPK Versions - 2.0.0 - 2.0.2, 1.7.0 - 1.9.2<br>BIG-IP Next CNF Versions - 2.0.0 - 2.1.0, 1.1.0 - 1.4.1<br>BIG-IP (all modules) - 17.5.0 - 17.5.1, 17.1.0 - 17.1.2, 16.1.0 - 16.1.6, 15.1.0 - 15.1.10 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://my.f5.com/manage/s/article/K000156733<br>• https://my.f5.com/manage/s/article/K44517780<br>• https://my.f5.com/manage/s/article/K000151658<br>• https://my.f5.com/manage/s/article/K000154647<br>• https://my.f5.com/manage/s/article/K000156944 |

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2022-50087, CVE-2025-37810, CVE-2025-37823, CVE-2025-37914, CVE-2025-38200, CVE-2025-38498, CVE-2025-38527) |
| 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 the affected system.<br>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64<br>Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/errata/RHSA-2025:18054 |

**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.**