# Advisory Alert

**Alert Number:** **AAA20250811** **Date:** **August 11, 2025**

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

**Information Classification Level** : TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **NetApp** | **Critical** | Linux Kernel Vulnerability |
| **Juniper** | **Critical** | Multiple Vulnerabilities |
| **IBM** | **Critical** | Multiple Vulnerabilities |
| **Dell** | **High** | Multiple Vulnerabilities |
| **F5** | **High**,<br>**Medium**,<br>**Low** | Multiple Vulnerabilities |
| **IBM** | **High**,<br>**Medium**,<br>**Low** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **NetApp** |
| Severity | **Critical** |
| Affected Vulnerability | Linux Kernel Vulnerability (CVE-2024-47685) |
| Description | NetApp has released a security update addressing a Linux Kernel Vulnerability that exists in their products.<br>**CVE-2024-47685** - Multiple NetApp products incorporate Linux kernel. Certain versions of Linux kernels are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information or Denial of Service (DoS).<br>NetApp advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Active IQ Unified Manager for VMware vSphere<br>E-Series SANtricity OS Controller Software 11.x<br>ONTAP tools for VMware vSphere 10<br>StorageGRID (formerly StorageGRID Webscale)<br>StorageGRID Baseboard Management Controller (BMC) - SG6060/SGF6024/SG100/SG1000<br>StorageGRID Baseboard Management Controller (BMC) - SG6160/SGF6112/SG110/SG1100 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://security.netapp.com/advisory/ntap-20250613-0011 |

| | |
|---|---|
| Affected Product | **Juniper** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2020-16156, CVE-2022-49395, CVE-2024-52005, CVE-2025-21587, CVE-2025-22869, CVE-2025-30698, CVE-2025-32414, CVE-2025-4447, CVE-2025-48734, CVE-2025-48976, CVE-2025-48988, CVE-2025-49125, CVE-2025-5283, CVE-2023-32732, CVE-2023-33953, CVE-2023-44487, CVE-2025-33097) |
| Description | Juniper has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause improper access control, memory buffering, embed arbitrary code.<br>Juniper advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Juniper Secure Analytics : 7.5.0 to 7.5.0 UP12 IF03. |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-U12-IF03?language=en_US |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2016-6293, CVE-2017-14952) |
| Description | IBM has released security updates addressing Multiple Vulnerabilities that exist in their products.<br>**CVE-2016-6293** - The uloc_acceptLanguageFromHTTP function in common/uloc.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ does not ensure that there is a '\0' character at the end of a certain temporary array, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long httpAcceptLanguage argument.<br>**CVE-2017-14952** - Double free in i18n/zonemeta.cpp in International Components for Unicode (ICU) for C/C++ through 59.1 allows remote attackers to execute arbitrary code via a crafted string, aka a "redundant UVector entry clean up function call" issue.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | IBM Db2 Server Versions - 10.5.0.0 - 10.5.0.11, 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7241823 |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-3596, CVE-2020-7105, CVE-2024-38428, CVE-2025-1795, CVE-2024-2398, CVE-2024-8096, CVE-2024-50602, CVE-2025-32414, CVE-2025-32415, CVE-2025-32728, CVE-2025-21605, CVE-2023-4738, CVE-2023-5344, CVE-2024-22667, CVE-2024-43802, CVE-2024-47814, CVE-2025-46836, CVE-2025-3576, CVE-2025-0395, CVE-2025-4802, CVE-2025-5222) |
| Description | Dell has released security updates addressing multiple vulnerabilities that exist in Dell Networking OS10. 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 Networking OS10 - Versions prior to 10.5.6.10 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000353631/dsa-2025-283-security-update-for-dell-networking-os10-vulnerabilities |

| | |
|---|---|
| Affected Product | **F5** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-24928, CVE-2024-56171, CVE-2024-43204, CVE-2025-24855, CVE-2024-55549) |
| Description | F5 has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause memory corruption, data modification, cache poisoning, session hijacking, cross-site scripting.<br>F5 advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Traffix SDC Versions - 5.2.0<br>BIG-IP (all modules) Versions - 17.5.0 - 17.5.1, 17.1.0 - 17.1.2, 16.1.0 - 16.1.6, 15.1.0 - 15.1.10<br>F5OS-A Versions - 1.8.0, 1.5.1 - 1.5.3<br>F5OS-C Versions - 1.8.0 - 1.8.1, 1.6.0 - 1.6.2 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://my.f5.com/manage/s/article/K000152930<br>• https://my.f5.com/manage/s/article/K000152932<br>• https://my.f5.com/manage/s/article/K000152924<br>• https://my.f5.com/manage/s/article/K000152944 |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2017-15422, CVE-2017-7868, CVE-2011-4599, CVE-2014-7923, CVE-2017-7867, CVE-2017-15396, CVE-2020-21913, CVE-2020-10531, CVE-2016-7415, CVE-2017-17484) |
| Description | IBM has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information discloser and denial of service.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | IBM Db2 Server Versions - 10.5.0.0 - 10.5.0.11, 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7241823 |

## 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.**