Advisory Alert

Alert Number: AAA20251009 **Date:** October 9, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
cPanel	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Use of Insufficiently Random Values vulnerability
Juniper Networks	**Critical**	Multiple Vulnerabilities
NetApp	**Critical**	Security Update
SUSE	**High**	Multiple Vulnerabilities
cPanel	**High**, **Medium**	Multiple Vulnerabilities
Juniper Networks	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
NetApp	**High**, **Medium**	Multiple Vulnerabilities
Check Point	**Medium**	Lack of TLS Validation Vulnerability
Red Hat	**Medium**	Multiple Vulnerabilities
Palo Alto Networks	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**cPanel**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-49844, CVE-2025-46817)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-49844** - Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free and potentially lead to remote code execution. The problem exists in all versions of Redis with Lua scripting. **CVE-2025-46817** - Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to cause an integer overflow and potentially lead to remote code execution The problem exists in all versions of Redis with Lua scripting. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following packages for EasyApache 4 versions prior to 25.31 • All versions of Redis through 6.2.19 • All versions of Valkey through 7.2.10 • All versions of Ruby Rack through 2.2.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-31-maintenance-and-security-release/

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 IBM Db2 Intelligence Center. **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. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Intelligence Center versions 1.1.0.0 - 1.1.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7247430

Affected Product	**Juniper Networks**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in Junos Space. These vulnerabilities could be exploited by malicious users to compromise the affected system. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of Junos Space
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Multiple-XSS-vulnerabilities-resolved-in-24-1R4-release • https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-24-1R4-release

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2024-47685)
Description	NetApp has released security updates addressing a vulnerability that exists in their products. **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. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere E-Series SANtricity OS Controller Software 11.x ONTAP tools for VMware vSphere 10 SnapCenter Plug-in for VMware vSphere/BlueXP Backup and Recovery for Virtual Machine StorageGRID (formerly StorageGRID Webscale)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250613-0011

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50154, CVE-2024-53168, CVE-2025-21791, CVE-2025-38477)
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 system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 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-202503498-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503497-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503496-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503485-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503482-1/

Affected Product	**cPanel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-61772, CVE-2025-61771, CVE-2025-61770, CVE-2025-46818, CVE-2025-46819)
Description	cPanel 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. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following packages for EasyApache versions prior to 25.31 • All versions of Redis through 6.2.19 • All versions of Valkey through 7.2.10 • All versions of Ruby Rack through 2.2.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-31-maintenance-and-security-release/

Affected Product	**Juniper Networks**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2015-1427, CVE-2015-5377, CVE-2018-3823, CVE-2018-3824, CVE-2018-3826, CVE-2018-3831, CVE-2018-17244, CVE-2018-17247, CVE-2021-4104, CVE-2021-22146, CVE-2021-42550, CVE-2021-44228, CVE-2021-44832, CVE-2021-45046, CVE-2021-45105, CVE-2025-11198, CVE-2025-52960, CVE-2025-52961, CVE-2025-59958, CVE-2025-59962, CVE-2025-59964, CVE-2025-59967, CVE-2025-59968, CVE-2025-59975, CVE-2025-59977, CVE-2025-60004, CVE-2025-60006, CVE-2025-60010)
Description	Juniper Networks 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, Data Modification, Privilege Escalation. Juniper Networks 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://supportportal.juniper.net/s/global-search/%40uri#sortCriteria=date%20descending&f-sf_primarysourcename=Knowledge&f-sf_articletype=Security%20Advisories

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-11250, CVE-2020-8565, CVE-2022-1471, CVE-2022-46175, CVE-2023-44487, CVE-2024-22243, CVE-2024-22259, CVE-2025-22868, CVE-2025-22870, CVE-2025-27789, CVE-2025-36244, CVE-2025-57810, CVE-2025-58754)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Server-Side Request Forgery, Denial of Service, Cross-Site Scripting, Elevation of Privilege, Remote Code Execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM DB2 Data Management Console version 3.1.12 IBM Db2 Intelligence Center versions 1.1.0.0 - 1.1.1.0 AIX versions 7.2 and 7.3 VIOS versions 3.1 and 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7247431 • https://www.ibm.com/support/pages/node/7247430 • https://www.ibm.com/support/pages/node/7245092

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42516, CVE-2024-36945, CVE-2023-39615, CVE-2024-50083, CVE-2024-50076)
Description	NetApp 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 and Data Modification. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9 ONTAP tools for VMware vSphere 10 SnapCenter Plug-in for VMware vSphere/BlueXP Backup and Recovery for Virtual Machine Active IQ Unified Manager for VMware vSphere E-Series SANtricity OS Controller Software 11.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250718-0013 • https://security.netapp.com/advisory/ntap-20250404-0006 • https://security.netapp.com/advisory/ntap-20250801-0009 • https://security.netapp.com/advisory/ntap-20250523-0010 • https://security.netapp.com/advisory/ntap-20250627-0003

Affected Product	**Check Point**
Severity	**Medium**
Affected Vulnerability	Lack of TLS Validation Vulnerability (CVE-2025-2028)
Description	Check Point has released security updates addressing a Lack of TLS Validation Vulnerability that exists in their products. **CVE-2025-2028** - Lack of TLS validation when downloading a visualization support data (CSV) file that includes mapping from IP addresses to countries used only for displaying country flags in logs. Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Check Point R81.10, R81.20 and R82
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk183349

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49985, CVE-2022-50087, CVE-2025-37914, CVE-2025-38200, CVE-2025-38211, CVE-2025-38449, 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. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:17570

Affected Product	**Palo Alto Networks**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-4615, CVE-2025-4614)
Description	Palo Alto Networks has released security updates addressing multiple vulnerabilities that exist in PAN-OS. **CVE-2025-4615** - An improper input neutralization vulnerability in the management web interface of the Palo Alto Networks PAN-OS software enables an authenticated administrator to bypass system restrictions and execute arbitrary commands. The security risk posed by this issue is significantly minimized when CLI access is restricted to a limited group of administrators. **CVE-2025-4614** - An information disclosure vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to view session tokens of users authenticated to the firewall web UI. This may allow impersonation of users whose session tokens are leaked. The security risk posed by this issue is significantly minimized when CLI access is restricted to a limited group of administrators. Palo Alto Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 11.2 - versions prior to 11.2.8 PAN-OS 11.1 - versions prior to 11.1.12 PAN-OS 10.2 - versions prior to 10.2.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2025-4615 • https://security.paloaltonetworks.com/CVE-2025-4614

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.