Advisory Alert

Alert Number: AAA20250711 **Date:** July 11, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Arbitrary Code Execution Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Citrix	**High**	Local Privilege Escalation Vulnerability
WatchGuard	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
Juniper	**High**, **Medium**	Multiple Vulnerabilities
Drupal	**High**, **Medium**	Multiple Vulnerabilities
cPanel	**Medium**	Multiple Vulnerabilities
Palo Alto	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-52950, CVE-2024-3596)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-52950** - An unauthenticated network-based attacker can exploit missing authorization checks on various API endpoints in the Juniper Security Director web UI. This flaw allows access to sensitive resources and potential configuration changes without proper authentication controls. **CVE-2024-3596** - A flaw in the RADIUS implementation within Junos OS and Junos OS Evolved allows an on-path attacker to forge valid RADIUS responses (e.g., change Access-Reject to Access-Accept) by exploiting weaknesses in the MD5-based Message-Authenticator field. This compromises authentication integrity, enabling unauthorized access. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS • All versions before 21.4R3-S11, • from 22.2 before 22.2R3-S7, • from 22.4 before 22.4R3-S7, • from 23.2 before 23.2R2-S4, • from 23.4 before 23.4R2-S5, • from 24.2 before 24.2R2-S1, • from 24.4 before 24.4R1-S3, 24.4R2 Junos OS Evolved • from 23.4-EVO before 23.4R2-S5-EVO, • from 24.2-EVO before 24.2R2-S1-EVO, • from 24.4-EVO before 24.4R1-S3-EVO, 24.4R2-EVO Juniper Security Director 24.4.1.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://supportportal.juniper.net/s/article/2025-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Vulnerability-in-the-RADIUS-protocol-for-Subscriber-Management-Blast-RADIUS-CVE-2024-3596?language=en_US • https://supportportal.juniper.net/s/article/2025-07-Security-Bulletin-Juniper-Security-Director-Insufficient-authorization-for-multiple-endpoints-in-web-interface-CVE-2025-52950?language=en_US

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2025-36038)
Description	IBM has released a security update addressing an arbitrary code execution vulnerability that exists in their product. **CVE-2025-36038** - IBM WebSphere Application Server could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Hybrid Edition - 5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7239362

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-48687, CVE-2023-42950, CVE-2024-10976, CVE-2024-10977, CVE-2024-10978, CVE-2024-10979, CVE-2024-1597, CVE-2024-21208, CVE-2024-21210, CVE-2024-21211, CVE-2024-21217, CVE-2024-21235, CVE-2024-25062, CVE-2024-36138, CVE-2024-47561, CVE-2024-47606, CVE-2024-54534, CVE-2024-7348, CVE-2025-0395, CVE-2025-0509, CVE-2025-1094, CVE-2025-21502, CVE-2025-21587, CVE-2025-23083, CVE-2025-30691, CVE-2025-30698, CVE-2025-4662, CVE-2025-6390, CVE-2025-6392)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Brocade 32Gb Fibre Channel SAN Switch for HPE Synergy - 9.1.0 through 9.2.2 • HPE B-series SN3600B Fibre Channel Switch - 9.1.0 through 9.2.2 • HPE B-series SN6600B Fibre Channel Switch - 9.1.0 through 9.2.2 • HPE B-series SN6650B Fibre Channel Switch - 9.1.0 through 9.2.2 • HPE B-series SN6700B Fibre Channel Switch - 9.1.0 through 9.2.2 • HPE B-series SN6750B Fibre Channel Switch - 9.1.0 through 9.2.2 • HPE SANnav Management Software SANnav base OS (OVA deployment) prior to Version 2.4.0a • HPE SN6750B 64Gb 48/128 48-port 64Gb Short Wave SFP56 Port Side Intake Integrated FC Switch - 9.1.0 through 9.2.2 • HPE SN8600B 4-slot SAN Director Switch - 9.1.0 through 9.2.2 • HPE SN8600B 8-slot SAN Director Switch - 9.1.0 through 9.2.2 • HPE SN8700B 4-slot SAN Director Switch - 9.1.0 through 9.2.2 • HPE SN8700B 8-slot SAN Director Switch - 9.1.0 through 9.2.2 • HPE Storage Fibre Channel Switch B-series SN3700B - 9.22
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04890en_us&docLocale=en_US

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49111, CVE-2022-49136, CVE-2022-49846, CVE-2022-50066, CVE-2023-1652, CVE-2023-52477, CVE-2023-52565, CVE-2023-52595, CVE-2023-52781, CVE-2023-52834, CVE-2024-26717, CVE-2024-35790, CVE-2024-35807, CVE-2024-35924, CVE-2024-36006, CVE-2024-36940, CVE-2024-39471, CVE-2024-41092, CVE-2024-41097, CVE-2024-43880, CVE-2024-46826, CVE-2024-56614, CVE-2025-22126, CVE-2025-37738, CVE-2025-37799)
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. 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-2025:10761 • https://access.redhat.com/errata/RHSA-2025:10701 • https://access.redhat.com/errata/RHSA-2025:10675 • https://access.redhat.com/errata/RHSA-2025:10671 • https://access.redhat.com/errata/RHSA-2025:10670 • https://access.redhat.com/errata/RHSA-2025:10669 • https://access.redhat.com/errata/RHSA-2025:10674

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5, 15.4 SUSE Linux Enterprise High Performance Computing 15 SP5, 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP5, ESPOS 15 SP4, LTSS 15 SP5, LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP5, 15-SP4 SUSE Linux Enterprise Micro 5.5, 5.4, 5.3 SUSE Linux Enterprise Micro for Rancher 5.4, 5.3 SUSE Linux Enterprise Real Time 15 SP5, 15 SP4 SUSE Linux Enterprise Server 15 SP5, 15 SP4 SUSE Linux Enterprise Server 15 SP5 LTSS, 15 SP4 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP5, 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502264-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502262-1/

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Local Privilege Escalation Vulnerability (CVE-2025-6759)
Description	Citrix has released a security update to address a local privilege escalation vulnerability in their products. A low-privileged user could exploit this vulnerability to gain SYSTEM privileges in the Windows Virtual Delivery Agent for CVAD and Citrix DaaS. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Citrix Virtual Apps and Desktops versions before 2503 Citrix Virtual Apps and Desktops 2402 LTSR CU2 and earlier versions of 2402 LTSR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694820&articleURL=Windows_Virtual_Delivery_Agent_for_CVAD_and_Citrix_DaaS_Security_Bulletin_CVE_2025_6759

Affected Product	**WatchGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-6946, CVE-2025-26466, CVE-2025-1547, CVE-2025-4106, CVE-2025-6999, CVE-2025-6947)
Description	WatchGuard 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, cross-site scripting, stack overflow, and request smuggling attacks. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Fireware OS - 12.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00009 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00011 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00013 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00010 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00014 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00012

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45332, CVE-2024-28047, CVE-2025-20054, CVE-2024-36350, CVE-2024-36357, CVE-2025-37101)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause information disclosure, denial-of-service, stack overflow, and privilege escalation. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Compute Scale-up Server 3200 – Prior to v1.60.88 HPE Superdome Flex 280 Server – Prior to v2.00.12 HPE Superdome Flex Server – Prior to v4.10.18 HPE Cray EX235a Accelerator Blade – Prior to 2.1.0 in HFP 25.2.1 HPE Cray EX235n Server – Prior to 1.5.3 in HFP 25.5.0 HPE Cray EX255a Accelerator Blade – Prior to 1.6.1 in HFP 25.3.0 (MI300PI v1.0.0.8) HPE Cray EX425 Compute Blade – Prior to 1.8.0 in HFP 25.5.0 HPE Cray EX4252 Compute Blade – Prior to 2.1.1 in HFP 25.5.0 HPE ProLiant XL225n Gen10 Plus 1U Node – Prior to 3.70_03-21-2025 HPE ProLiant XL645d Gen10 Plus Server – Prior to 3.70_03-21-2025 in HFP 25.5.0 HPE ProLiant XL675d Gen10 Plus Server – Prior to 3.70_03-21-2025 in HFP 25.5.0 HPE Cray XD675 – Prior to 3.02.03 in Firmware Pack 2025.05.00 HPE OneView for VMware vCenter with Operations Manager and Log Insight – All versions prior to v11.7 HPE Compute Ops Management – All versions prior to v1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04868en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04871en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04869en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04892en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04876en_us&docLocale=en_US

Affected Product	**Juniper**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Juniper 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?language=en_US#sortCriteria=date%20descending&f-sf_articletype=Security%20Advisories&numberOfResults=50

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-7392, CVE-2025-7393)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-7392** - A moderately critical XSS flaw exists in the Cookies Addons "Embed Iframe" sub-module, where insufficient filtering of user-supplied content in text fields with iframe permissions allows an attacker with the right access to inject malicious scripts. **CVE-2025-7393** - The module included some protection against brute force attacks on the login form, however they were incomplete. An attacker could bypass the brute force protection allowing them to potentially gain access to an account. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cookies Addons – Versions greater than 1.0.0 and less than 1.2.4 Mail Login project - Versions greater than 3.0.0 but less than 3.2.0, Versions greater than or equal to 4.0.0 but less than 4.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2025-087 • https://www.drupal.org/sa-contrib-2025-088

Affected Product	**cPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-52891, CVE-2025-1735, CVE-2025-6491, CVE-2025-1220)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of PHP 8.1 through 8.1.32. All versions of PHP 8.4 through 8.4.8. All versions of ModSecurity 2 through 2.9.10. All versions of PHP 8.3 through 8.3.22. All versions of PHP 8.2 through 8.2.28.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-22-maintenance-and-security-release/

Affected Product	**Palo Alto**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0141, CVE-2025-0140, CVE-2025-0139)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-0139** - An incorrect privilege assignment vulnerability in Palo Alto Networks Autonomous Digital Experience Manager allows a locally authenticated low privileged user on macOS endpoints to escalate their privileges to root. **CVE-2025-0140** - An incorrect privilege assignment vulnerability in the Palo Alto Networks GlobalProtect App on macOS and Linux devices enables a locally authenticated non administrative user to disable the app even if the GlobalProtect app configuration would not normally permit them to do so. **CVE-2025-0141** - An incorrect privilege assignment vulnerability in the Palo Alto Networks GlobalProtect App on enables a locally authenticated non administrative user to escalate their privileges to root on macOS and Linux or NT AUTHORITY\SYSTEM on Windows. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Autonomous Digital Experience Manager - Versions prior to 5.6.7 on macOS GlobalProtect App (macOS) • Versions 6.3.0 through 6.3.3-h1 • Versions 6.2.0 through 6.2.8-h2 • All versions of 6.1.x and 6.0.x GlobalProtect App (Linux) • Versions 6.2.0 through 6.2.8 • All versions of 6.1.x and 6.0.x GlobalProtect App (Windows) • Versions 6.3.0 through 6.3.3-h1 (6.3.3-c650) • Versions 6.2.0 through 6.2.8-h2 (6.2.8-c243) • All versions of 6.1.x and 6.0.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://securityadvisories.paloaltonetworks.com/CVE-2025-0139 • https://securityadvisories.paloaltonetworks.com/CVE-2025-0140 • https://securityadvisories.paloaltonetworks.com/CVE-2025-0141

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.