Advisory Alert

Alert Number: AAA20260402 **Date:** April 2, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Synology	**Critical**	Buffer Overflow Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
Drupal	**High**	Authentication Bypass Vulnerability
WatchGuard	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
NetApp	**High, Medium**	Multiple Vulnerabilities
Cisco	**High, Medium**	Multiple Vulnerabilities
HPE	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Joolma	**High, Medium**	Multiple Vulnerabilities
Ubuntu	**High, Medium**	Multiple Vulnerabilities
cPanel	**High, Medium, Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
Synology	**Medium**	Remote Code Injection Vulnerability
SonicWall	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Synology**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-32746)
Description	Synology has released a security update addressing a vulnerability that exists in their products. **CVE-2026-32746:** telnetd in GNU inetutils through 2.7 allows an out-of-bounds write in the LINEMODE SLC (Set Local Characters) suboption handler because add_slc does not check whether the buffer is full. Synology advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	DSM 7.3 – Versions prior to 7.3.2-86009-3 DSM 7.2.2 – Versions prior to 7.2.2-72806-8 DSM 7.2.1 – Versions prior to 7.2.1-69057-11 DSMUC 3.1 – Versions prior to 3.1.5-23082
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_26_03

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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 systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Unisphere for PowerMax Virtual Appliance — Versions prior to 9.2.4.20 Solutions Enabler — Versions prior to 9.2.4.14 Solutions Enabler Virtual Appliance — Versions prior to 9.2.4.14 Solutions Enabler — Versions prior to 10.3.0.1 Dell PowerMax EEM 5978 — Versions prior to 5978.720.720.11249 Dell PowerMax EEM 10.3.1.0 — Versions prior to 10.3.1.0 Patch 11248 Dell PowerMaxOS 5978 — Versions prior to 5978.720.720.11249 Dell PowerMax OS 10.3.0.1 — Versions prior to 10.3.0.1 Patch 11248 Dell PowerProtect Data Manager – Versions prior to 20.1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000446607/dsa-2026-153-dell-powermaxos-dell-powermax-eem-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtualappliance-dell-unisphere-360-dell-solutionsenabler-and-dell-solutionsenabler-virtualappliance-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000447277/dsa-2026-158-security-update-dell-powerprotect-data-manager-for-multiple-security-vulnerabilities

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20093, CVE-2026-20160)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-20093:** This vulnerability is due to incorrect handling of password change requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to bypass authentication, alter the passwords of any user on the system, including an Admin user, and gain access to the system as that user. This vulnerability could allow an unauthenticated, remote attacker to bypass authentication and gain access to the system as Admin. **CVE-2026-20160:** This vulnerability is due to the unintentional exposure of an internal service. An attacker could exploit this vulnerability by sending a crafted request to the API of the exposed service. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. This vulnerability could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected SSM On-Prem host. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Cisco Integrated Management Controller (IMC) • 5000 Series Enterprise Network Compute Systems (ENCS) • Catalyst 8300 Series Edge uCPE • UCS C-Series M5 and M6 Rack Servers in standalone mode • UCS E-Series Servers M3 • UCS E-Series Servers M6 Cisco Smart Software Manager On-Prem (SSM On-Prem)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-cli-execution-cHUcWuNr

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-5343)
Description	Drupal has released a security update addressing a vulnerability that exists in their product. **CVE-2026-5343:** The SAML SSO - Service Provider module enables you to perform SAML-protocol-based single-sign-on (SSO) on a Drupal site. The module doesn't sufficiently block access, leading to a authentication bypass vulnerability. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SAML SSO - Service Provider module – Versions prior to 3.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-031

Affected Product	**WatchGuard**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-3987, CVE-2026-23268, CVE-2026-23269)
Description	WatchGuard has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-3987:** A path traversal vulnerability in the Fireware OS Web UI on WatchGuard Firebox systems may allow a privileged authenticated remote attacker to execute arbitrary code in the context of an elevated system process. **CVE-2026-23268:** An unprivileged local user can load, replace, and remove profiles by opening the apparmorfs interfaces, via a confused deputy attack, by passing the opened fd to a privileged process, and getting the privileged process to write to the interface. This does require a privileged target that can be manipulated to do the write for the unprivileged process, but once such access is achieved full policy management is possible and all the possible implications that implies: removing confinement, DoS of system or target applications by denying all execution, by-passing the unprivileged user namespace restriction, to exploiting kernel bugs for a local privilege escalation **CVE-2026-23269:** In the Linux kernel, the following vulnerability has been resolved: apparmor: validate DFA start states are in bounds in unpack_pdb Start states are read from untrusted data and used as indexes into the DFA state tables. The aa_dfa_next() function call in unpack_pdb() will access dfa->tables[YYTD_ID_BASE][start], and if the start state exceeds the number of states in the DFA, this results in an out-of-bound read. WatchGuard advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Fireware OS 2025.1.x (Prior to 2026.2) • T115-W, T125, T125-W, T145, T145-W, T185, M295, M395, M495, M595, M695 Fireware OS 12.x (Prior to 12.12) • T20, T25, T40, T45, T55, T70, T80, T85, M270, M290, M370, M390, M470, M570, M590, M670, M690, M440, M4600, M4800, M5600, M5800, Firebox Cloud, Firebox NV5, FireboxV Other • Dimension v2.3 • WebBlockerServer v2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00008 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00009

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22768, CVE-2026-22767)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. **CVE-2026-22768:** Dell AppSync, version(s) 4.6.0, contain(s) an UNIX Symbolic Link (Symlink) Following vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering. **CVE-2026-22767:** Dell AppSync, version(s) 4.6.0, contain(s) an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell AppSync – Versions prior to 4.6.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000446965/dsa-2026-163-security-update-for-dell-appsync-vulnerabilities

Affected Product	**NetApp**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-69420, CVE-2026-22795)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-69420:** A type confusion vulnerability exists in the TimeStamp Response verification code where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid or NULL pointer dereference when processing a malformed TimeStamp Response file. An application calling TS_RESP_verify_response() with a malformed TimeStamp Response can be caused to dereference an invalid or NULL pointer when reading, resulting in a Denial of Service. The functions ossl_ess_get_signing_cert() and ossl_ess_get_signing_cert_v2() access the signing cert attribute value without validating its type. When the type is not V_ASN1_SEQUENCE, this results in accessing invalid memory through the ASN1_TYPE union, causing a crash. **CVE-2026-22795:** An invalid or NULL pointer dereference can happen in an application processing a malformed PKCS#12 file. An application processing a malformed PKCS#12 file can be caused to dereference an invalid or NULL pointer on memory read, resulting in a Denial of Service. A type confusion vulnerability exists in PKCS#12 parsing code where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid pointer read. The location is constrained to a 1-byte address space, meaning any attempted pointer manipulation can only target addresses between 0x00 and 0xFF. This range corresponds to the zero page, which is unmapped on most modern operating systems and will reliably result in a crash, leading only to a Denial of Service. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ONTAP 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20260204-0005 • https://security.netapp.com/advisory/ntap-20260204-0006

Affected Product	**Cisco**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20085, CVE-2026-20087, CVE-2026-20088, CVE-2026-20089, CVE-2026-20090, CVE-2026-20042, CVE-2026-20041, CVE-2026-20174, CVE-2026-20094, CVE-2026-20095, CVE-2026-20096, CVE-2026-20097, CVE-2026-20151, CVE-2026-20155)
Description	Cisco 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. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Cisco Integrated Management Controller (IMC) • 5000 Series Enterprise Network Compute Systems (ENCS) • Catalyst 8300 Series Edge uCPE • UCS C-Series M5 and M6 Rack Servers in standalone mode • UCS E-Series Servers M3 & M6 • UCS S-Series Storage Servers in standalone mode Cisco Smart Software Manager On-Prem (SSM On-Prem) Cisco Evolved Programmable Network Manager (EPNM) Cisco Nexus Dashboard • Version 4.1 • Versions prior to 3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-priv-esc-xRAnOuO8 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-improp-auth-mUwFWUU3 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-xss-A2tkgVAB • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-cbid-5YqkOSHu • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-ssrf-NAen4O7r • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndi-afw-rJuRC5dZ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-3hKN3bVt

Affected Product	**HPE**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-30513, CVE-2025-31944, CVE-2025-32007, CVE-2025-32467, CVE-2025-27572, CVE-2025-27940)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE ProLiant Compute DL320 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute DL340 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute ML350 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute DL360 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute DL380 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute DL380a Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute DL580 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute XD230 - Prior to v1.60_01-09-2026 HPE Alletra Storage Server 4210 - Prior to v1.60_01-09-2026 HPE Synergy 480 Gen12 Compute Module - Prior to v1.60_01-09-2026 HPE ProLiant DL110 Gen11 - Prior to v2.80_01-29-2026 HPE ProLiant DL320 Gen11 Server - Prior to v2.80_01-29-2026 HPE ProLiant ML350 Gen11 Server - Prior to v2.80_01-29-2026 HPE ProLiant DL360 Gen11 Server - Prior to v2.80_01-29-2026 HPE ProLiant DL380 Gen11 Server - Prior to v2.80_01-29-2026 HPE ProLiant DL380a Gen11 - Prior to v2.80_01-29-2026 HPE ProLiant DL560 Gen11 - Prior to v2.80_01-29-2026 HPE ProLiant ML110 Gen11 - Prior to v2.80_01-29-2026 HPE Alletra 4110 - Prior to v2.80_01-29-2026 HPE Alletra 4120 - Prior to v2.80_01-29-2026 HPE Alletra 4140 - Prior to v2.80_01-29-2026 HPE Compute Edge Server e930t - Prior to v2.80_01-29-2026
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05007en_us&docLocale=en_US#supported-software-versions-only-impacted-versions-2

Affected Product	**IBM**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38129, CVE-2025-38248, CVE-2025-40064, CVE-2025-68800, CVE-2026-23074, CVE-2025-69419, CVE-2025-12818, CVE-2025-71085, CVE-2026-23001, CVE-2026-23097, CVE-2025-14915, CVE-2025-14917, CVE-2026-1561)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QRadar – Versions 7.5.0 - 7.5.0 UP15 IBM WebSphere Hybrid Edition – Version 5.1 IBM WebSphere Application Server Liberty – Version 17.0.0.3 - 26.0.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7268179 • https://www.ibm.com/support/pages/node/7268390 • https://www.ibm.com/support/pages/node/7268386 • https://www.ibm.com/support/pages/node/7268382

Affected Product	**Joomla**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23899, CVE-2026-23898, CVE-2026-21632, CVE-2026-21631)
Description	Joomla has released security updates addressing multiple vulnerabilities that exist in their product. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Joomla advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Joomla! CMS – Versions 4.0.0-5.4.3 & 6.0.0-6.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://developer.joomla.org/security-centre/1032-20260306-core-improper-access-check-in-webservice-endpoints.html • https://developer.joomla.org/security-centre/1031-20260305-core-arbitrary-file-deletion-in-com-joomlaupdate.html • https://developer.joomla.org/security-centre/1030-20260304-core-xss-vectors-in-various-article-title-outputs.html • https://developer.joomla.org/security-centre/1029-20260303-core-xss-vector-in-com-associations-comparison-view.html

Affected Product	**Ubuntu**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23074, CVE-2026-23060, CVE-2025-21735, CVE-2024-46777, CVE-2021-47254, CVE-2021-47145, CVE-2021-47142)
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu – Versions 14.04 & 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8142-1 • https://ubuntu.com/security/notices/USN-8143-1

Affected Product	**cPanel**
Severity	**High,** Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-27654, CVE-2026-27784, CVE-2026-32647, CVE-2026-27651, CVE-2026-28753, CVE-2026-28755, CVE-2026-21637, CVE-2026-21710, CVE-2026-21713, CVE-2026-21714, CVE-2026-21717, CVE-2026-21715, CVE-2026-21716, CVE-2026-27135)
Description	cPanel has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	EasyApache v25.52
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38154, CVE-2025-38180, CVE-2026-23001, CVE-2026-23209)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:6310

Affected Product	**Synology**
Severity	**Medium**
Affected Vulnerability	Remote Code Injection Vulnerability (CVE-2026-5129)
Description	Synology has released a security update addressing a vulnerability that exists in their products. **CVE-2026-5129**: Synology has released a security update for the Mail Station package in DSM to address a vulnerability which allows remote authenticated users to read or write limited files. Synology advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Mail Station for DSM 7.3 – Versions prior to 30000001.3.19-20332 Mail Station for DSM 7.2.2 – Versions prior to 30000001.3.19-20332 Mail Station for DSM 7.2.1 – Versions prior to 30000001.3.19-20332
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_26_04

Affected Product	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-3468, CVE-2026-3469, CVE-2026-3470)
Description	SonicWall has released a security update addressing a vulnerability that exists in their products. **CVE-2026-3468**: A stored Cross-Site Scripting (XSS) vulnerability has been identified in the SonicWall Email Security appliance due to improper neutralization of user-supplied input during web page generation, allowing a remote authenticated attacker as admin user to potentially execute arbitrary JavaScript code. **CVE-2026-3469:** A denial-of-service (DoS) vulnerability exists due to improper input validation in the SonicWall Email Security appliance, allowing a remote authenticated attacker as admin user to cause the application to become unresponsive. **CVE-2026-3470:** A vulnerability exists in the SonicWall Email Security appliance due to improper input sanitization that may lead to data corruption, allowing a remote authenticated attacker as admin user could exploit this issue by providing crafted input that corrupts application database. SonicWall advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ES Appliance 5000, 5050, 7000, 7050, 9000, VMWare and Hyper-V • Versions 10.0.34.8215, 10.0.34.8223 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0002

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.