VSP N400, N600, N800 Release Notes SVOS 7.4.1, DKCMAIN 83-06-27-x0/00, SVP 83-06-28-x0/00, NAS OS 15.5.8424.05, SMU 15.5.8424.05

Contents

About this document

This document (RN-830627-M245-00, December 2025) provides information about the firmware for Hitachi Virtual Storage Platform (VSP) N400, N600, N800, including new features and functions and changes.

Intended audience

This document is intended for customers and Hitachi Vantara partners who license and use VSP N400, N600, N800 storage systems.

Getting help

The Hitachi Vantara Support Website is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website. For additional contact methods, go to https://support.hitachivantara.com/en/contact-support.html.

Hitachi Vantara Community is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Accessing product downloads

Product software, drivers, and firmware downloads are available on the Hitachi Vantara Support Website: https://support.hitachivantara.com.

Log in and select Download Products and Updates to access the most current downloads, including important updates that may have been made after the release of the product.

About this release

This document describes the differences between the following versions:

Product	Firmware/software	New version	Previous version
SVOS	-	7.4.1	Same as left
VSP N800	DKCMAIN	83-06-27-60/00	83-06-26-60/00
	SVP	83-06-28-60/00	83-06-27-60/00
VSP N400, N600	DKCMAIN	83-06-27-40/00	83-06-26-40/00
	SVP	83-06-28-40/00	83-06-27-40/00
NAS Module	NAS OS	15.5.8424.05	15.4.8321.05
	SMU	15.5.8424.05	15.4.8321.05

Supported features and functions

The following tables list the new features and functions in this release. For additional details (for example, affected components, operational notes), contact your Hitachi Vantara representative.

No.	Title and description
1	Support for OpenJDK 11.0.28 OpenJDK 11.0.28 is supported to address the following vulnerabilities. - CVE-2025-50059 - CVE-2025-30749 - CVE-2025-50106 - CVE-2025-30761 - CVE-2025-30754
2	Support for Apache 2.4.65, OpenSSL 3.0.17, apr-1.7.6, and libexpat-2.7.1 Apache 2.4.65, OpenSSL 3.0.17, apr-1.7.6, and libexpat-2.7.1 are supported to address the following vulnerabilities. Apache 2.4.64 - CVE-2024-42516 - CVE-2024-43204 - CVE-2024-43394 - CVE-2024-47252 - CVE-2025-23048 - CVE-2025-49630 - CVE-2025-49812 - CVE-2025-53020 Apache 2.4.65 - CVE-2025-54090 OpenSSL 3.0.17 None apr-1.7.6 None libexpat-2.7.1 - CVE-2024-8176

No.	Title and description
3	Support for logback 1.3.15 and 1.5.18 and slf4j 2.0.17 logback 1.3.15 and 1.5.18, and slf4j 2.0.17 are supported to address the following vulnerabilities, though the function applicable to the vulnerabilities is not used so that microcode is not affected. CVE-2023-6378 CVE-2023-6481 CVE-2024-12798 CVE-2024-12801 CVE-2018-8088
4	Support for CCI Ver. 01-82-03/00 Modified function: - The paircreate command is modified to use the physical capacity when confirming free capacity of pools to which the pool automatic expansion function is not enabled by running the paircreate command.
5	Support for including reset processing time of Open host in monitoring target Reset processing time of Open host is included as the monitoring target for MP operating rate.

NAS OS and SMU firmware

No.	Title and description
1	NFSv4.1 Preserve Unlinked Support • VSP One File 32 / 34 / 38 • HNAS 5200 / 5300 There is a longstanding client-side mechanism in NFS to deal with the situation where one host process has an NFS file in use ('open') and another process - on the same host - requests deletion of that file. Instead of the file being immediately deleted, the NFS client renames the file in question using a temporary name (usually of the form .nfsXXXXX) - and tracks all the processes using the file, only finally removing it once the last process using it is finished with it. This is known as “silly rename”. The main drawback is that silly rename is limited to requests made within the same host; files opened by an NFS client from another host are not recognised and could potentially lead to stale file handle issues on the client. Furthermore, if a client is interrupted (eg abruptly disconnected or crashes) all files that have been renamed will remain on the server until they are manually deleted. In NFSv4.1 a new mechanism - called preseved-unlinked - was provided to allow this to be dealt with server-side. If enabled, an NFS server will include the PRESEVED_UNLINKED flag set when replying to a client’s OPEN4 request, telling NFS clients that also support the option that the server will guarantee any open file handles can still provide access to the file until the last reference to it is

	released. From 15.5, the server supports - on a per-EVS basis via the use of nfsv41-preserve-unlinked* commands - this mechanism. It is disabled on all EVSs by default, and it is generally advised to leave it disabled unless interoperability is required with an application (whose data is accessed via NFS) that is known to depend upon the preserve unlinked functionality. It has been found that the Apache Kafka has this requirement. As only NFSv4.1 provides support for this mechanism, the server requires nfs-max-supported-version be set to 4.1 before use. If preserve-unlinked is enabled with an earlier NFS version set, it will have no effect. There are currently a number of known restrictions and best practices for the usage of this feature: • In order to maintain resilience regarding the state of preserved files over EVS migrations - either manual or automatic (due to node reboot or interruption) - it is recommended that nfsv4-state-reclaim is also enabled on EVSs when preserve-unlinked is enabled. • It is not recommended to have NFSv4 as an audited protocol for file systems on an EVS where preserve-unlinked is enabled. If both features are in use on an EVS, a comprehensive audit log of transactions over NFSv4.x cannot be guaranteed. • It is recommended that this feature be enabled before connecting NFS clients to exports on a given EVS. Similarly, it is recommended that all clients be disconnected from all exports on an EVS before the feature is disabled. • Due to the way this feature interacts with the Third-Party Migration (also known as Universal Migration) feature, it is currently not recommended to use it on EVSs where preserve-unlinked has been enabled. Not all NFS clients support this feature, so may continue to use ‘silly rename’.
2	New events: directory reached a size threshold or became full A new event is now logged when a directory reaches, by default, 80% of its maximum size. Another new event is logged when it fills up. The new events provide information about the absolute path to the directory from the root of file system. More information is available in the man page for the max-dir-size command.
3	Time protection improvements • VSP One File 32 / 34 / 38 • HNAS 5200 / 5300 The Time Protection feature is supported on VSP One File and HNAS 5000 series since release 15.4.8321.05. Improvements in this release include a new cluster state monitor which generates a severe event if the time protection state of the cluster nodes is inconsistent, better handling of time protection state during reinstall and other events to attract administrative attention when certain configuration changes may affect or be affected by the time protection feature.
4	Native REST API HNAS native REST API v9 enhanced to add management of additional functional areas of the HNAS product – for full details refer to the latest version of the Hitachi NAS REST API Reference

	Guide MK-92HNAS100. v7 and v8 versions of the native REST API are retained and still supported.
5	SMU CentOS Stream 9 A virtual SMU can now be deployed on the CentOS Stream 9 operating system.

Fixed problems

The following tables list the bug fixes in this release. For additional details (for example, conditions of occurrence, probability), contact your Hitachi Vantara representative.

No.	Category	Severity	Title and symptoms
1	Universal Replicator	High	I/O error in open configuration After performing a suspend operation for a UR pair with data writing Enabled on the S-VOL, if combining with or deleting the P-VOL was performed while a WR I/O was being issued to the SVOL, an I/O error might occur in the open configuration.
2	Open	High	Controller blockage when receiving non-standards frame When receiving a non-ANSI standards RSCN frame from an FC switch, a controller board blockage occurred. SSB=32FE Reference code=3073
3	Global-active device	High	GAD pair with P-VOL and S-VOL in PSUE(Block) The pair status and I/O mode of some GAD pairs in a CTG became PSUE (Block) on both the P-VOL and S-VOL. SSB=FC83 or FC85 was logged.
4	Dynamic Provisioning, Dynamic Tiering, Thin Image	Medium	One-byte space deleted or added in pool name when running REST API For a value returned by running the following Configuration Manager REST API, a one-byte space of poolName attribute was deleted, or unnecessary one-byte spaces were added. GET <base URL >/v1/objects/pools GET <base URL >/v1/objects/pools/<Object ID > Example of the failure: Correct: "pool 0 - DF0" Incorrect: "pool0 - DF0"

No.	Category	Severity	Title and symptoms
5	Universal Replicator	Medium	Failure of initial copy/resync operation in UR-UR multi-target configuration In a UR-UR multi-target configuration, initial copy failed (SSB=8F04), or a resync operation failed and the pair became in Suspending status (SIM=DC1XYY, SSB=8F04).
6	Open	Medium	Maintenance Utility vulnerability due to insufficient authentication information protection Maintenance Utility had a vulnerability due to insufficient authentication information protection.
7	Open	Medium	Privilege escalation vulnerability in storage system management software A vulnerability (CVE-2025-9480) in the storage system management software could allow privilege escalation, which might affect the management and maintenance of the storage system.
8	Global-active device	Medium	Abend of pair deletion by copy group with KARD40097-E output When running an API to delete pairs by copy group, if the number of pairs in a single copy group exceeded 1,000, the operation ended abnormally with KART40097-E output.
9	Open	Medium	Random success or Failure of REST API without specifying Content-Type When a REST API that required a request body was run without specifying Content-Type, the API might succeed or fail randomly. Whether it succeeded or failed changed with each restart of SVP/MPC. KART40046-E Note: This refers to products that ran API without specifying Content-Type, such as HSPC.
10	Open	Medium	Unable to login to Maintenance Utility due to password expiration If a password was changed before enabling user account policy, the date when the password was changed was saved so that the password might be expired after enabling user account policy. In this case, a login to Maintenance Utility might fail due to password expiration. At that time, Maintenance Utility message 32061-205006 was displayed. In addition, the following error messages were reported: Storage Navigator: Failed to login CCI: User authentication has failed(stat = 2)

No.	Category	Severity	Title and symptoms
			REST API: HTTP Status Code 401(Unauthorized) Embedded CCI: Permission denied Export Tool2: 2 (Termination code)
11	Command Control Interface	Medium	Wrong value returned for pairevtwait -s/-ss For the pairevtwait -s/-ss command, 0 (normal end) might be returned wrongly.
12	Dynamic Provisioning, dedupe and compression	Medium	Failure of disabling capacity saving and status change Disabling capacity saving for a virtual volume could not be complete. The capacity saving status did not change but remained Rehydrating.
13	Thin Image	Medium	Abend of TI S-VOL operation with SSB=9792/9720 logged Assigning a TI S-VOL, releasing TI S-VOL assignment, or changing a TI S-VOL ended abnormally and SSB=9792 and 9720 might be logged.
14	Open	Medium	Performance degradation/temporary SM blockage/failure of controller board replacement Due to repeated ownership migration of LDEVs or creation/deletion of LDEVs or virtual volumes, one or more of the following phenomena occurred. (1) Performance degradation (2) Temporary blockage of SM (3) Failure of controller board replacement
15	Open	Medium	Failure of displaying Maintenance Utility login window The Maintenance Utility login window was not displayed, and a message that said "This page can't be reached." was displayed.
16	Global-active device, TrueCopy, Universal Replicator	Medium	Invalid value/unnecessary information output in audit log When TC, UR, or GAD pair force deletion was performed for an LDEV from the LDEVs window on Storage Navigator, invalid values were output in audit logs as follows. (1) TC pair force deletion from the LDEVs window - S-VOL (Port-G-ID-LUN): CLI-A-00 was always output. - Type: P-VOL was always output. (2) UR pair force deletion from the LDEVs window - S-VOL (Port-G-ID-LUN): CL1-A-00 was always output. - MirrorID: 0x00 was always output.

No.	Category	Severity	Title and symptoms
			- S/N: An empty string was always output. - CTLID: 0 was always output. (3) GAD pair force deletion from the LDEVs window - S-VOL (Port-G-ID-LUN): CLI-A-00 was always output. - SSID_S: 0x0000 was always output. - MirrorID: 0x00 was always output. - Invisible: Disable was always output.
17	Global-active device	Medium	Failure of GAD pair resynchronization with SSB=FB54 logged After volumes on MCU or RCU of GAD pairs in a CTG were deleted by partial force deletion, and then the GAD pairs were suspended (including swap suspension) per CTG (this procedure was different from the usual operating procedure), if the GAD pairs were resynchronized while the number of GAD pairs in the CTG differed between MCU and RCU, the operation failed with SSB=FB54 logged.
18	Drive	Medium	Drive media error or PIN due to sustained high workload on drives A drive media error (SIM=434xxx) (*1) or PIN (SIM=FF4xxx) (*2) may occur due to sustained high workload on DKS2O-H (firmware: 00-7F-09) drives. If drive media errors occur frequently, a drive blockade may occur. If multiple drive blockades occur in the same parity group (PG), the redundancy of the PG is lost and the LDEV is blocked. (*1) Drive media error may be caused by unrecovered read error (SSB=A403). (*2) PIN may occur if an unrecovered read error occurs on a different drive during the drive copy operation.
19	Open	Medium	CHB and MP blockage at data transfer error While a data transfer time-out occurred frequently for a reason on the host side, when write data was received, a data transfer error caused by a T10DIF error occurred many times and a CHB and an MP were blocked. SSB=B2FF, B3DC, B3DD SIM=3073XX, FFF3XX, 3080XX, 2130XX, 680001
20	Open	Medium	Maintenance Utility login failure after controller board replacement After controller board replacement, an attempt to log in to Maintenance Utility might fail with Maintenance Utility message 32061-205006 displayed.

No.	Category	Severity	Title and symptoms
21	Open	Medium	Failure of exporting GUM audit log file with message 34062-203403 Exporting the GUM audit log file might fail with Maintenance Utility message 34062-203403 reported.
22	Open	Medium	LAN error due to depletion of memory used by GUM While a storage system was operating, the memory used by GUM was depleted and SIM=7D01XY was reported, which resulted in an internal LAN error or an inability to perform maintenance operations.
23	Global-active device	Medium	GAD pair failure suspension after suspending operation Suspending a GAD pair by an operation failed with SSB=FC39 logged and Storage Navigator message 06205 208036 (W) displayed, and the pair was suspended due to failure with SSB=D1EA, E5C2 logged on MCU and SSB=D374 logged on RCU.
24	Global-active device	Medium	Suspension/deletion/host I/O unavailable after GAD pair suspension following PS OFF While a PAIR status GAD pair belonging to a consistency group existed, when the GAD pair was suspended by an operation immediately after PS OFF for one of storage systems (still PS OFF was in process), the GAD pair status remained Suspending (the pair status was PAIR on CCI, the consistency group status was Suspending on Storage Navigator). (In this status, suspension/normal deletion operation and host I/Os for the GAD pair were not available.)
25	Open	Medium	MP blockage with SSB=1644 logged When the control information for Open read commands became invalid, an incorrect memory access occurred and an MP was blocked. SSB=1644
26	Open	Medium	Unable to automatically correct difference in number of managed cache resources When a difference in the number of cache management resources occurred between the two controller boards, the difference was only automatically corrected on one of the controller boards, but not on both boards. As a result, one or more of the following phenomena occurred. (1) Performance degradation (2) Blockage of one area of SM (3) Controller board replacement failure

No.	Category	Severity	Title and symptoms
			SSB=137F SIM=FFEE0X Maintenance Utility message 30762-208299, 30762-208330
27	Adaptive Data Reduction, dedupe and compression	Medium	Pinned slot caused by concurrent CTL failure and power outage or CTL failure during PS ON When a CTL failure and a power outage occurred simultaneously, or when a CTL failure was detected during PS ON, a pinned slot might occur. However, because the pinned slots were readable and writable with no impact on the storage system, it was not necessary to immediately take recovery actions. SSB=8019 SIM=FF40XX
28	Open	Medium	No password expiration notification sent to maintenance user Due to password expiration, an attempt to log in to Maintenance Utility made with the maintenance user resulted in Maintenance Utility message 32061-205006. In addition, the following error messages were reported: Storage Navigator message: Failed to login. CCI: User authentication has failed(stat = 2)
29	Open	Medium	Login failure due to memory shortage Because multiple processing were run at a time for storing the GUM trace data, memory shortage occurred and a login attempt failed as a result. In addition, SIM=7D01XY and 7D00XY were frequently reported. - Maintenance Utility message: 32061-205006 - Storage Navigator message: Failed to login. - CCI message: User authentication has failed(stat = 2)
30	Dynamic Provisioning, dedupe and compression	Medium	Unable to reduce virtual volume usage rate with SSB=AF51, AFC0, AFE1 logged The following phenomena occurred at the same time. Phenomenon 1 Running a Write Same/ Unmap command or performing zero data page reclamation could not decrease the usage rate of a virtual volume. Phenomenon 2 SSB=AF51, AFC0, AFE1 were logged continuously.

No.	Category	Severity	Title and symptoms
31	Open	Medium	WCHK1 with SSB=3F4D logged and MP blockage When a storage system of a different model than the storage system of MPC or SVP in use was connected, the communication I/F size of the storage system of MPC/SVP was used for communicating to the connected storage system, so that WCHK1 occurred with SSB=3F4D logged on the connected storage system, and then MP blockage might occur.
32	Adaptive Data Reduction	Medium	Cache write pending rate remaining at 60% When a specific ADR volume existed, the CWP rate might not drop below 60%. SIM=3073XX SSB=01FF (Byte:0x2d-0x2f = 0x020b05)
33	Open	Low	Vulnerability CVE-2025-7377 in Virtual Storage Platform REST API Virtual Storage Platform REST API had the vulnerability (CVE-2025-7377) of storing token in a session
34	Audit Log	Low	Incorrect "uid" and "from" display in audit log In the audit log (operation name: Automatic LDAP Password change) that was output when external authentication from SVP and then the operation of Changing the user information used in searches of the external authentication server set for a storage system were performed, "uid" and "from" were displayed as follows. uid = null ("uid" should be a user ID) from = , (a comma) ("from" should be an IP address) The target REST API request line PATCH <base URL>/v1/objects/external-authentication-server-settings/instance
35	Storage Navigator	Low	Authentication error when starting Maintenance Utility from MPC When a user who had been logged in to MPC performed a password-related operation and then started Maintenance Utility from MPC, an internal error (SVP message SVP0029E, error code=05BF) occurred.
36	Global-active device, ShadowImage, TrueCopy, Universal Replicator	Low	Insufficient information for failure investigation The information necessary for investigating a failure that occurred at a customer site was not sufficient so that the investigation took a long time.

No.	Category	Severity	Title and symptoms
37	Dynamic Provisioning	Low	Unable to stop pool shrinking Even though an operation for stopping pool capacity shrinking was performed, the pool shrinking did not stop.
38	Open	Low	Incorrect storage system status display in Maintenance Utility at all MP blockage When all MPs were blocked, the storage system status displayed in Maintenance Utility should be Failed, but it remained as Ready.
39	Hitachi Command Suite	Low	Returning KARD40098 when deleting many pairs When the following REST API was run in an environment where about 1,000 to 3,000 deletion target pairs existed, KART40098-E might be returned even though the deletion processing ended normally. * The number of target pairs when the problem occurred varied depending on the storage system performance. The problem occurred when deleting device groups on the remote side took more than 10 minutes. DELETE remote-mirror-copygroups/<object ID>
40	Open	Low	Incorrectly 100% write hit rate displayed during controller board blockage During controller board blockage, the write hit rate shown on the monitor was incorrectly 100%.
41	Open	Low	SSB=998B logged during high load random write I/O During high load random write I/Os, SSB=998B might be logged.
42	Open	Low	Displaying Ready even when incorrect storage system is connected If MPC or SVP was connected to an incorrect storage system, maintenance operations could not be performed so that Communication in the Service Status window of the Storage Device List should be Warning, but Ready was displayed.
43	Universal Replicator	Low	Incorrect time-out detection with SSB=8E52 logged In the copy processing in a UR configuration, a time-out was incorrectly detected and SSB=8E52 was logged.
44	Open	Low	Inappropriate storage system status change in Maintenance Utility When all MPs are blocked, Failed was displayed for the status of the storage system in Maintenance Utility, but after a while, it was changed to Ready.

NAS OS and SMU firmware

Issue ID	Severity	Description
D140185	C	Fix an issue with named pipe buffer management that can occur when the buffer wraps
D161183	C	Reinstated the restriction to upgrade/downgrade from/to at most one major version step at a time, to maintain compatibility.
D161689	C	An unlikely unscheduled instability due to the scale of credential augmentation on a heavily laden system is made less likely.
D161690	C	The cluster-unconfigure command can now safely be used in cases where the last remaining node is not node 1. This has been seen with hardware rolling upgrade but this is not the only scenario that results in this issue.
D161702	C	CentOS 9 : expat-2.5.0-4.el9 Reference Information: 2024-A-0694 CVE-2024-50602 CentOS 9 : gcc-11.5.0-5.el9 Reference Information: 2025/02/13 CVE-2020-11023 CentOS 9 : kernel-5.14.0-527.el9 Reference Information: CVE-2024-41035, CVE-2024-42244 CentOS 9 : kernel-5.14.0-533.el9 Reference Information: CVE-2024-38564, CVE-2024-40914, CVE-2024-43898, CVE-2024-45009, CVE-202445010, CVE-2024-45020, CVE-2024-46695, CVE-2024-46711, CVE-2024-46828, CVE-2024-47675, CVE-2024-47685, CVE-2024-47700, CVE-2024-47703, CVE-202447745, CVE-2024-49888, CVE-2024-49948, CVE-2024-49968, CVE-2024-50014, CVE-2024-50015, CVE-2024-50018, CVE-2024-50033, CVE-2024-50093, CVE-2024- 50099, CVE-2024-50110, CVE-2024-50127, CVE-2024-50130, CVE-2024-50142, CVE-2024-50154, CVE-2024-50186, CVE-2024-50191, CVE-2024-50262

Issue ID	Severity	Description
		CentOS 9 : kernel-5.14.0-536.el9 Reference Information: CVE-2024-36011, CVE-2024-49950, CVE-2024-50029, CVE-2024-50044, CVE-2024-50067, CVE-2024-50077, CVE-2024-50078, CVE-2024-50125, CVE-2024-50148, CVE-2024-50255 CentOS 9 : kernel-5.14.0-539.el9 Reference Information: CVE-2023-52917, CVE-2024-49951, CVE-2024-50299 CentOS 9 : kernel-5.14.0-542.el9 Reference Information: CVE-2022-48989, CVE-2024-46673, CVE-2024-49870, CVE-2024-49975, CVE-2024-50046, CVE-2024-50106, CVE-2024-50109, CVE-2024-50121, CVE-2024-50256 CentOS 9 : kernel-5.14.0-547.el9 Reference Information: CVE-2024-44945, CVE-2024-50258, CVE-2024-53096, CVE-2024-53104, CVE-202453113, CVE-2024-53118, CVE-2024-53140 CentOS 9 : kernel-5.14.0-554.el9 Reference Information: CVE-2024-40964, CVE-2024-41037, CVE-2024-41069, CVE-2024-42074, CVE-202442089, CVE-2024-42097, CVE-2024-42298, CVE-2024-43818, CVE-2024-43896, CVE-2024-44954, CVE-2024-46793, CVE-2024-46798, CVE-2024-46849, CVE-202446862, CVE-2024-46863, CVE-2024-50007, CVE-2024-50011, CVE-2024-50103, CVE-2024-50104, CVE-2024-50105, CVE-2024-50160, CVE-2024-50292, CVE-2024- 53045, CVE-2024-53150, CVE-2024-53197, CVE-2024-56532, CVE-2024-56533 CentOS 9 : kernel-5.14.0-559.el9 Reference Information: CVE-2022-48674, CVE-2023-52526, CVE-2024-53232, CVE-2024-56562, CVE-2024-56568, CVE-2024-56624, CVE-2024-56668, CVE-2024-56669, CVE-2024-57929 CentOS 9 : kernel-5.14.0-565.el9 Reference Information: CVE-2024-53208, CVE-2024-53237, CVE-2024-56653, CVE-2024-57879

Issue ID	Severity	Description
		CentOS 9 : kernel-5.14.0-529.el9 Reference Information: CVE-2024-42322, CVE-2024-46786, CVE-2024-49974, CVE-2024-50038, CVE-202450107 CentOS 9 : kernel-5.14.0-572.el9 Reference Information: CVE-2022-49623, CVE-2024-46689, CVE-2024-50060, CVE-2024-53052, CVE-2024-56690, CVE-2024-56709, CVE-2025-21785 CentOS 9 : kernel-5.14.0-573.el9 Reference Information: CVE-2022-49269, CVE-2023-52922, CVE-2024-53241, CVE-2024-56631, CVE-202457807, CVE-2025-1272, CVE-2025-21694, CVE-2025-21786 CentOS 9 : libxml2-2.9.13-9.el9 Reference Information: 2025-A-0123 CVE-2025-24928 CentOS 9 : microcode_ctl-20241112-1.el9 Reference Information: CVE-2024-21820, CVE-2024-21853, CVE-2024-23918, CVE-2024-23984 CentOS 9 : microcode_ctl-20250211-1.el9 Reference Information: CVE-2023-34440, CVE-2023-43758, CVE-2024-24582, CVE-2024-28047, CVE-2024-28127, CVE-2024-29214, CVE-2024-31068, CVE-2024-31157, CVE-2024-36293, CVE-2024-37020, CVE-2024-39279, CVE-2024-39355 CentOS 9 : openssh-8.7p1-45.el9 Reference Information: 2025-A-0126 CVE-2025-26465
D161778	C	Fix an issue that might, vary rarely, result in server instability whilst performing software profiling
D161850	C	A deadlock vulnerability in the Bali LDAP stack has been addressed.
D161889	C	Kerberos clients requesting no-mutual-authentication (eg RHEL9 NFS clients) are no longer denied access when using AES keys.
D162169	C	Fixed potential instability caused by a race condition when an NFSv4.1

Issue ID	Severity	Description
		DESTROY_CLIENTID4 request is being handled and the client is being restarted at the same time.
D162217	C	Improved hit count and hit rate calculation in ldap-cache-stats/nis-cache-stats
D163063	C	The implementation limit on the number of checkpoints per file system is raised from 2 Gi - 1. No limit is known before 4 Gi - 1.
D160515	D	Added monitoring of the Logical Volume Management on the chassis drives of applicable platforms (VSP One File 34/38).
D161858	D	The maximum WORM retention time is now set to the year 2106.
D161879	D	Additional details are now returned via the REST API for system drivers, allowing the storage array type to be identified
D161920	D	The REST API ignoreBestPractice variable did not consider all situations when creating a multi-tier storage pool
D162040	D	Fixed errors with the smu-restore/smu-restore-with-password command line scripts on the SMU running on CentOS Stream 9.
D162046	D	Increases the maximum number of NFSv4.x open files per node up to 1.5 M, interpolating this maximum number based on the heap size and some possible customer configuration adjustments.
D162074	D	Using the REST API, API keys that are restricted by EVS only, are no longer allowed to manipulate management users or API keys - to use those functions, API keys need to be created to specifically allow the operations.
D162111	D	Debian dla-4018 : libruby2.7 - security update Reference Information: None provided. Debian dla-4050 : bind9 - security update Reference Information: 2025-A-0071 CVE-2024-11187 Debian dla-4057 : openssh-client - security update Reference Information: CVE-2025-26465 Debian dla-4061 : libtasn1-6 - security update Reference Information: CVE-2024-12133 Debian dla-4063 : gnutls-bin - security update Reference Information:

Issue ID	Severity	Description
		CVE-2024-12243 Debian dla-4064 : libxml2 - security update Reference Information: 2024-A-0067-S, 2025-A-0123 CVE-2017-9047, CVE-2022-49043, CVE-2023-39615, CVE-2023-45322, CVE-2024- 25062, CVE-2024-56171, CVE-2025-24928, CVE-2025-27113 Debian dla-4065 : krb5-admin-server - security update Reference Information: CVE-2025-24528 Debian dla-4069 : emacs - security update Reference Information: CVE-2023-28617, CVE-2024-53920, CVE-2025-1244 Debian dla-4074 : libmariadb-dev - security update Reference Information: CVE-2025-21490 Debian dla-4082 : libruby2.7 - security update Reference Information: CVE-2025-27219, CVE-2025-27220, CVE-2025-27221 Debian dla-4085 : tzdata - security update Reference Information: None provided. Debian dla-4087 : idle-python3.9 - security update Reference Information: CVE-2022-0391, CVE-2025-0938, CVE-2025-1795
D162134	D	Running "autoinquiry-config -t smb2 on" on the File32 platform will fail with the message "SMB2.x/3.x autoinquiry is not supported on this model"
D162228	D	smu-getlogs now includes some configuration files that were sometimes previously excluded on the grounds of being more than ~half a year old.

Issue ID	Severity	Description
D162241	D	The REST API version has been increased from v9.4 to v9.5, for changes see the updated API reference document
D162256	D	A set-for-evs variable, ldap-netgroup-lookup-disable-per-evs, can be used to disable the use of LDAP for netgroup queries on a more granular basis than the cluster-wide ldap-netgroup-lookup-enable setting.
D162286	D	cluster-show --all command now shows time protection information.
D162306	D	The version of Tomcat used by the SMU has been upgraded to 9.0.102, fixing this vulnerability: CVE-2025-24813
D162308	D	Time Protection CLI commands now operate across all online nodes in the cluster.
D162344	D	Per-node time protection REST APIs have been retired.
D162396	D	SMTP can now e-mail log events up to 1023 bytes long.
D162410	D	NFSv4.1 preserve unlinked is now supported as an optional feature, configurable per EVS. This is intended to improve interoperability with Kafka, avoiding some sillyrename derived issues that are now prevented at least for RHEL8.7/RHEL 9.1 clients.
D162449	D	Debian dla-4092 : libcap-dev - security update Reference Information: 2025-A-0134 CVE-2023-2602, CVE-2023-2603, CVE-2025-1390 Debian dla-4095 : intel-microcode - security update Reference Information: CVE-2023-34440, CVE-2023-43758, CVE-2024-24582, CVE-2024-28047, CVE-2024-28127, CVE-2024-29214, CVE-2024-31068, CVE-2024-31157, CVE-2024-36293, CVE-2024-37020, CVE-2024-39279, CVE-2024-39355 Debian dla-4096 : amqp-tools - security update Reference Information: CVE-2023-35789 Debian dla-4097 : vim - security update Reference Information: 2022-B-0049-S, 2022-B-0058-S, 2023-B-0016-S, 2023-B-0018-S, 2023-B-0033-S, 2023-B-0066-S, 2023-B-0074-S 2023-A-0526-S, 2024-A-0618-S CVE-2021-3872, CVE-2021-4019, CVE-2021-4173, CVE-2021-4187, CVE-2022-0261, CVE-2022-0351, CVE-2022-0359, CVE-2022-0361, CVE-2022-0392, CVE2022-0417, CVE-2022-0572, CVE-2022-1616, CVE-2022-1785,

Issue ID	Severity	Description
		CVE-2022-1897, CVE-2022-1942, CVE-2022-2000, CVE-2022-2129, CVE-2022-2304, CVE-2022-3099, CVE-2022-3134, CVE-2022-3324, CVE-2022-4141, CVE-2023-0054, CVE2023-1175, CVE-2023-2610, CVE-2023-4738, CVE-2023-4752, CVE-2023-4781, CVE-2023-5344, CVE-2024-22667, CVE-2024-43802, CVE-2024-47814 Debian dla-4117 : atop - security update Reference Information: 2025-A-0210 CVE-2025-31160 Debian dla-4128 : libglib2.0-0 - security update Reference Information: CVE-2025-3360 Debian dla-4130 : login - security update Reference Information: CVE-2023-4641, CVE-2023-29383 Debian dla-4138 : distro-info-data - security update Reference Information: None provided. Debian dla-4143 : glibc-doc - security update Reference Information: 2025-A-0062 CVE-2025-0395 Debian dla-4145 : expat - security update Reference Information: 2024-A-0694-S CVE-2024-50602 Debian dla-4146 : libxml2 - security update Reference Information: 2024-A-0229-S, 2025-A-0293 CVE-2025-32414, CVE-2025-32415 Debian dla-4154 : libmariadb-dev - security update Reference Information:

Issue ID	Severity	Description
		CVE-2023-52969, CVE-2023-52970 Debian dla-4156 : openssh-client - security update Reference Information: 2025-A-0258 CVE-2025-32728 Debian dla-4163 : bundler - security update Reference Information: CVE-2021-43809, CVE-2023-28755, CVE-2025-27221 Debian dla-4170 : intel-microcode - security update Reference Information: CVE-2024-28956, CVE-2024-43420, CVE-2024-45332, CVE-2025-20012, CVE-2025- 20054, CVE-2025-20103, CVE-2025-20623, CVE-2025-24495 Debian dla-4175 : libbson-1.0-0 - security update Reference Information: CVE-2021-32050, CVE-2023-0437, CVE-2024-6381, CVE-2024-6383, CVE-20250755 Debian dla-4176 : libcrypto1.1-udeb - security update Reference Information: 2025-A-0127-S CVE-2024-13176 Debian dla-4181 : glibc-doc - security update Reference Information: 2025-A-0062 CVE-2025-4802 Debian dla-4182 : syslog-ng - security update Reference Information: CVE-2024-47619 Debian dla-4195 : krb5-admin-server - security update Reference Information: CVE-2025-3576

Issue ID	Severity	Description
		Debian dla-4202 : net-tools - security update Reference Information: CVE-2025-46836 Debian dla-4208 : libmariadb-dev - security update Reference Information: CVE-2025-30693, CVE-2025-30722 Debian dla-4213 : curl - security update Reference Information: 2023-A-0153-S, 2023-A-0531-S CVE-2023-27534 Debian dla-4217 : icu-devtools - security update Reference Information: CVE-2025-5222
D162496	D	Debian dla-4104 : freetype2-demos - security update Reference Information: CVE-2025-27363 Debian dla-4105 : tzdata - security update Reference Information: None provided.
D162572	D	Correctable memory errors now cause a SEVERE event to be logged, the severity was previously 'WARNING'.
D162608	D	Debian dla-4133 : wget - security update Reference Information: CVE-2024-38428
D162715	D	Apache Tomcat 9.0.0.M1 < 9.0.104 multiple vulnerabilities Reference Information: 2025-A-0313-S CVE-2025-31650, CVE-2025-31651 Apache Tomcat 9.0.0.M1 < 9.0.105 Reference Information: 2025-A-0389 CVE-2025-46701

Issue ID	Severity	Description
		Apache Tomcat 9.0.0.M1 < 9.0.106 multiple vulnerabilities Reference Information: CVE-2025-48976, CVE-2025-48988, CVE-2025-49124, CVE-2025-49125 Apache Tomcat 9.0.0.M1 < 9.0.107 multiple vulnerabilities Reference Information: 2025-A-0478 CVE-2025-52434, CVE-2025-52520, CVE-2025-53506
D162716	D	CentOS 9 : bzip2-1.0.8-10.el9 Reference Information: 2020-A-0482 CVE-2019-12900 CentOS 9 : kernel-5.14.0-575.el9 Reference Information: CVE-2024-58005, CVE-2025-21791 CentOS 9 : kernel-5.14.0-578.el9 Reference Information: CVE-2024-58007, CVE-2025-21726, CVE-2025-21796, CVE-2025-21864 CentOS 9 : kernel-5.14.0-580.el9 Reference Information: CVE-2022-49627, CVE-2025-21702, CVE-2025-21765, CVE-2025-21790, CVE-202521891 CentOS 9 : kernel-5.14.0-582.el9 Reference Information: CVE-2024-52332, CVE-2024-53216, CVE-2024-54191, CVE-2025-21714, CVE-202521768, CVE-2025-21847, CVE-2025-22005 CentOS 9 : kernel-5.14.0-583.el9 Reference Information: CVE-2025-21745, CVE-2025-21837 CentOS 9 : kernel-5.14.0-585.el9 Reference Information:

Issue ID	Severity	Description
		CVE-2024-53229, CVE-2025-21756, CVE-2025-21844, CVE-2025-37749, CVE-202537785 CentOS 9 : kernel-5.14.0-587.el9 Reference Information: CVE-2022-3424, CVE-2022-49648, CVE-2024-50301, CVE-2024-57901, CVE-2024-57902, CVE-2025-21863, CVE-2025-21962, CVE-2025-21964, CVE-2025-22055 CentOS 9 : kernel-5.14.0-598.el9 Reference Information: CVE-2022-49846, CVE-2024-58088, CVE-2025-21693, CVE-2025-21728, CVE-202521759, CVE-2025-21851, CVE-2025-21853, CVE-2025-22066, CVE-2025-22104, CVE-2025-23134, CVE-2025-37805, CVE-2025-37891, CVE-2025-37919, CVE-202537934, CVE-2025-37941, CVE-2025-37979 CentOS 9 : kernel-5.14.0-601.el9 Reference Information: CVE-2022-49788, CVE-2025-21829, CVE-2025-21919 CentOS 9 : libarchive-3.5.3-5.el9 Reference Information: 2024-A-0834 CVE-2025-25724 CentOS 9 : libxml2-2.9.13-10.el9 Reference Information: CVE-2025-6021, CVE-2025-49794, CVE-2025-49796 CentOS 9 : ncurses-6.2-12.20210508.el9 Reference Information: CVE-2022-29458, CVE-2023-29491
D162847	D	Java has been updated to version 8u452-b09, addressing vulnerabilities up to and including those disclosed in: * https://openjdk.org/groups/vulnerability/advisories/2025-04-15, which calls out CVE- 2025-21587, CVE-2025-30698, CVE-2025-30691, CVE-2024-54534, CVE-202447606 https://openjdk.org/groups/vulnerability/advisories/2025-01-21, which calls out CVE2025-21502

Issue ID	Severity	Description
D162855	D	Debian dla-4235 : sudo - security update Reference Information: 2025-A-0465 CVE-2025-32462 Debian dla-4251 : libxml2 - security update Reference Information: 2024-A-0067-S CVE-2024-34459, CVE-2025-6021, CVE-2025-6170, CVE-2025-49794, CVE-202549796 Debian dla-4259 : systemd - security update Reference Information: CVE-2025-4598
D162952	D	Java has been upgraded to 8u462-b08, addressing vulnerabilities up to and including those disclosed in: * https://openjdk.org/groups/vulnerability/advisories/2025-07-15, which calls out CVE- 2025-50059, CVE-2025-30749, CVE-2025-50106, CVE-2025-30761, CVE-2025-30754
D161202	E	Minor usability improvements to ethernet-link-config
D161710	E	A snapshot schedule deletion via the REST API was not checking if the API key used to authenticate the request was restricted from performing operations on the EVS hosting the filesystem. A check is now done before the schedule is deleted.
D161760	E	Record management audit log servers and connection status when collecting diagnostics.
D161926	E	A cause of "All peers are not included in the graph, one or more are missing" while getting diagnostics has been addressed.
D161979	E	Time protection status is now a part of diagnostic's showall.txt
D162009	E	When creating a multi-tier storage pool using the REST API, not all tier details were returned. This should no longer be the case.
D162110	E	The SNMP MIB file has been updated to include up to date contact info
D162464	E	An issue, which prevented a default NTP server from being added on boot, has been fixed.
D162588	E	tzdata rpm was updated to tzdata-2025b-1.el9.noarch

Copyrights and licenses