Vertiv™ Next Connect

Release Notes

VERSION 1.6, NOVEMBER 11, 2025

Release Notes Section Outline

1. Updates to This Release (Version 1.6)

November 11, 2025

This version of Vertiv™ Next Connect focuses on added features, performance enhancements, platform updates, bug fixes, and security updates.

Features and Enhancements

- Cloud
    - Feature – Vertiv™ Liebert® GXT5 UPS Firmware Update via Vertiv™ Liebert® IntelliSlot™ RDU101 (Single/Bulk)
        - Supports the following Vertiv™ Liebert® GXT5 UPS model configurations (sub-models):
            - VRLA UPS 500-3KVA (LV, HV, I)
            - VRLA UPS 5KVA-10KVA (HV, I)
            - VRLA UPS 5KVA-10KVA (MV)
            - VRLA UPS 15KVA-20KVA (MV)
            - VRLA UPS 16KVA-20KVA (I)
            - Lithium-Ion UPS 1000-3000VA (LV, I)
            - Lithium-Ion UPS 5KVA-10KVA (MV)
    - Firmware update disabled when Vertiv™ Liebert® GXT5 UPS in-alarm
    - Feature – Vertiv™ Liebert® IntelliSlot™ RDU120 Monitoring Support
    - Feature – Vertiv™ Liebert® IntelliSlot™ RDU120 Provisioning Support (Single/Bulk)
        - Create Admin User, Enable SNMP, Setup Networking
        - Push Configuration Files
        - Communication Card Firmware Update
        - Discovery (Card/Device)
    - Feature – Support Device Configuration via SNMP Writes for all device models (includes third-party)
    - Feature – Allow reboot of card/communication controller for Vertiv™ Liebert® IntelliSlot™/ Vertiv™ Geist™ (PowerIT)
    - Improvement – Traps now compliant with RFC 3584
    - Improvement – Upgraded to Angular 19
    - Improvement – Added 'Latest' Flag to firmware versions
    - Improvement – List Performance Improvements (Reduce Real-Time Updates)

    - Affects the following lists:
      - Agents
      - Customers
      - Devices
      - Groups
      - Partners
      - Sites
      - Users
  - Improvement – Added “ongoing maintenance” banner
  - Improvement – Removed system groups, removed requirement to assign devices to groups, added uniqueness check
  - Improvement – Product name changed from “Vertiv™ Environet™ Connect” to “Vertiv™ Next Connect”
  - Improvement – Allow ‘equals’ conditions for traps
- Device Support
  - New Devices (UPS) -
    - Vertiv™ Liebert® GXE3 1000IRT2UXL
    - Eaton UPS 9PXM-12KVA
    - Eaton UPS 5P750
    - APC Smart UPS SRT 1000
  - New Configuration Example – Vertiv™ Geist™ Upgradeable 2.0 (GU2) PDUs turning on/off outlets
  - New Configuration Example – Vertiv™ Liebert® IntelliSlot™ RDU120 configurations
  - Improvement – Allow all users to request templates

Bug Fixes

- Improved sync of Serial Number for monitored devices.
- Added system model number.
- Fixed issue with default templates not always being assigned after discovery.
- Fixed notifications for completed discovery scans.
- Fixed issue where deleting devices did not always delete from the agent.
- Fixed issue where the device was not saved after creating a group.
- Fixed issue with downloading agent logs.
- Fixed issue with filtering by date in logs.
- Fixed issue with excessive logging for some devices.
- Fixed issue where some agents are not displayed in lists.
- Reduced sensitivity of online/offline determination.
- Fixed issues with sorting/filtering for all lists.
- Fixed issue with removing/adding groups.
- Fixed discrepancies with groups displayed in list and device views.
- Fixed issues where the groups dashboard saves when no changes are made.
- Fixed issue where the user is unable to add group pins to the plan widget.
- Fixed issue where dashboard graphs can load without data.
- Fixed issue where traps can be received by the agent but not processed.
- Fixed issue with batching alarms.

- Fixed issue with excessive notifications for cleared alarms.
- Fixed issues with manual clearing of alarms.
- Fixed issues where changes to access are not propagated immediately.
- Fixed issue with firmware version not populated or populated incorrectly.
- Fixed issue where “false failures” are reported for successful updates.
- Improved error-handling when taking provisioning action without credentials.
- Fixed logging/notification issues with provisioning.
- Fixed issue where provisioning sections are intermittently unavailable.
- Fixed issue where users were unable to perform bulk firmware updates on devices.
- Fixed issues with bulk pushing SNMP write configurations.
- Fixed issue with networking configuration on Vertiv™ Geist™ GU2 PDUs.
- Fixed issue where provisioning action was shown in progress after failure.
- Improved filtering of models when uploading configuration files.
- Fixed issue where columns were not removed from some reports.
- Fixed issue with discrepancies in how dates are displayed in reports.
- Fixed issues where some PDF exports do not include all elements.
- Fixed issue where the login button needed to be clicked twice in some scenarios.
- Fixed login issue with user registration.
- Fixed images in some email notifications.
- Fixed issues with loading the user list.
- Removed unused hyperlinks on the login page.
- Fixed issue where notification settings did not load with expected defaults for new users.
- Fixed issue where the session expires without an indication or during long operations.
- Fixed license notification issue.
- Fixed license calculation (allocation/deallocation) issues.
- Fixed issues where the user could exceed license limits.
- Fixed issues where users could take add/edit actions after the license expired.
- Fixed cosmetic issues with button placement, list display, and spacing.
- Fixed navigation / redirect issues.

Security Updates

REFERENCE NUMBER	DESCRIPTION
-	Audited API endpoints to ensure that authorization is consistently enforced
-	Upgraded Microsoft.Build.Tasks.Core
CVE-2022-40897	Python Packaging Authority (PyPA) setup tools before 65.5.1 allow remote attackers to cause a denial of service via HTML in a crafted package or custom PackageIndex page. There is a Regular Expression Denial of Service (ReDoS) in package_index.py.
CVE-2022-40898	An issue discovered in Python Packaging Authority (PyPA) Wheel 0.37.1 and earlier allows remote attackers to cause a denial of service via attacker-controlled input to the wheel CLI.
CVE-2024-6345	A vulnerability in the package_index module of pypa/setuptools versions up to 69.1.1 allows for remote code execution via its download functions. These functions, which are used to download packages from URLs provided by users or retrieved from package index servers, are susceptible to code injection. If these functions are exposed to user-

REFERENCE NUMBER	DESCRIPTION
	controlled inputs, such as package URLs, they can execute arbitrary commands on the system. The issue is fixed in version 70.0.
CVE-2025-2907	jsPDF is a library to generate PDFs in JavaScript. Prior to 3.0.1, user control of the first argument of the addImage method results in CPU utilization and denial of service. If given the possibility to pass unsanitised image URLs to the addImage method, a user can provide a harmful data URL that results in high CPU utilization and denial of service. Other affected methods are HTML and addSvgAsImage. The vulnerability was fixed in jsPDF 3.0.1.

2. Version 1.5 Update Information

March 25, 2025

This version of Vertiv™ Next Connect focuses on added features, performance enhancements, platform updates, bug fixes, and security updates.

Features and Enhancements

- Cloud
  - Feature – UPS Fleet Management Summary Report
  - Feature – UPS Detailed Report
  - Feature – Template Builder (**Internal**, Desktop Only): Includes configurable discovery rules, import for polled data and traps from CSV, points/traps editor, dashboard layout, copying (points, traps, template), delete (points, traps, template), import/export for deployment
  - Feature – Training Videos added to Support
  - Improvement – Improved throughput performance via Stream Analytics
  - Improvement – Added additional license options (trials, 5-year terms, five devices)
  - Improvement – API Rate Limiting
- Local Agent
  - Improvement – Updated EFlow to Latest Version 1.5.1.28104 LTS
  - Improvement – Agents now use discovery rules from templates available to the customer
  - Improvement – New reminder screen for checking VM settings
  - Improvement – Improved refresh rate for agent version, IP, and logs
  - Improvement – Downloads recommend the best agent. Added a reminder for the nested virtualization of Windows agents
- Device Support
  - New Device (Modular UPS) –
    - Vertiv™ Liebert® APM UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
    - Vertiv™ Liebert® EXM UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - New Device (UPS) –
    - Vertiv™ Liebert® EXL S1 UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
    - Vertiv™ Liebert® EXS UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
    - Vertiv™ Liebert® GXE 2kVA UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card

- New Device (Thermal) –
  - Vertiv™ Liebert® Mini-Mate2/Vertiv™ Liebert® DM with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Liebert® Mini-Mate 10.5 Capacity Indoor, Water/Glycol-cooled or Air-cooled Condensing Unit with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Liebert® XDU 1350A Coolant Distribution Unit
  - Vertiv™ Liebert® DS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Liebert® PDX with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
- New Configuration Example (Modular UPS) –
  - Vertiv™ Liebert® APM UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Liebert® APS UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Liebert® EXM with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
- New Configuration Example (UPS) –
  - Vertiv™ Edge UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Liebert® EXL S1 UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Liebert® EXS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Liebert® GXE 2kVA UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
- Improvement – Updated existing UPS templates to include data required by reports.
- Improvement – Added support for battery technology on UPS models (VRLA, Lithium-Ion). Created new templates for UPSs that support multiple battery technologies.

Bug Fixes

- Improved the display of lists on tablets.
- Implemented cosmetic fix to align allocation options with license options.
- Confirmed support for provisioning/firmware update across multiple subnets.
- Removed duplicate logging of numeric values.
- Removed logging of adding Vertiv™ Liebert® IntelliSlot™ Unity and Vertiv™ Liebert® IntelliSlot™ RDU101 cards for monitoring.
- Restored access to my profile page for technician and operator users.
- Fixed issue where new users are unable to access the product (are bounced to the home screen).
- Fixed issues where new entities were not showing after creation.
- Fixed issue where partner was not deleted after deleting from the 3-dots menu.
- Fixed issues where entities reappeared after being deleted.
- Fixed issue where some entities could not be deleted as expected.
- Fixed issue where alarms for deleted devices were not cleared.
- Fixed issue where editing a device reset the template to the default.
- Fixed issue where changing a device template could cause the local agent to crash.
- Fixed issues with partner/customer uniqueness checks.
- Fixed issue where new local agents were created as disabled.
- Fixed edge case where entities could be bulk deleted despite an empty search.
- Fixed issue where log pages would fail to load with a server 500 error.
- Fixed invalid links in the audit log.
- Fixed issue where the names of points that change are not logged.
- Fixed logging issue where “agent modified by system” entries were flooding logs.
- Fixed logging of EFlow version upgrades.

- Fixed scaling issue where wrong UoM and/or scale were applied to readings for some devices.
- Fixed clearing of numeric alarms.
- Fixed issue where device firmware was not shown for the Vertiv™ Liebert® GXT5 UPS.
- Fixed issue where Vertiv™ Liebert® Intellislot™ devices were discovered as “Unknown.”
- Fixed issues where devices were incorrectly discovered as “Integrated.”
- Fixed intermittent failures when device discovery, pushing configuration files, and firmware.
- Fixed issue where the template was not correctly assigned during the discovery scan.
- Fixed issue where IPv4 addresses were missing from the device report for integrated communication devices.
- Fixed issue where users could not see configuration files authored by their organization.
- Fixed issue where the MFA button was not active in some scenarios.
- Fixed issue with sorting by date on lists.
- Fixed issue where some pages crashed on mobile.
- Fixed issue where license expiration emails were not sent (warning, expired).
- Fixed issue with duplicate and missing license options.
- Fixed issue where the license expiration ribbon could not be dismissed.
- Fixed intermittent issue where alarms and SMS messages are not sent in some cases.
- Fixed additional areas where clicking edit took the user off the current tab.
- Fixed cosmetic issue where images were not correctly displayed in password expiration and license expiration emails.
- Fixed cosmetic issue with the label for critical low alarms.

Security Updates

REFERENCE NUMBER	DESCRIPTION
-	User Passwords now expire after 90 days (by default).
-	Users may not reuse their previous three passwords when setting a new password.
-	Fixed issue where password changes were audit-logged without encryption.
-	Fixed multiple permissions issues where users could take unauthorized actions.
-	Fixed displayed message for disabled users (“This user account is disabled”).
-	All endpoints updated to require authorization.
-	Removed connection details from agent install logs.
CVE-2017-0247	A denial-of-service vulnerability exists when ASP.NET Core fails to properly validate web requests. **NOTE: Microsoft has not commented on third-party claims that the issue is with the TextEncoder.EncodeCore function in the System.Text.Encodings. Web package in ASP.NET Core Mvc before 1.0.4 and 1.1.x before 1.1.3 allows remote attackers to cause a denial of service by leveraging failure to correctly calculate the length of 4-byte characters in the Unicode Non-Character range.**
CVE-2017-0248	Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, and 4.7 allow an attacker to bypass Enhanced Security Usage taggings when they present a certificate that is invalid for a specific use, known as the ".NET Security Feature Bypass Vulnerability."
CVE-2017-0249	An elevation of privilege vulnerability exists when the ASP.NET Core fails to sanitize web requests properly.

REFERENCE NUMBER	DESCRIPTION
CVE-2017-0256	A spoofing vulnerability exists when the ASP.NET Core fails to sanitize web requests properly.
CVE-2018-8292	An information disclosure vulnerability exists in .NET Core when authentication information is inadvertently exposed during a redirect, also known as the ".NET Core Information Disclosure Vulnerability." This affects .NET Core 2.1, .NET Core 1.0, .NET Core 1.1, and PowerShell Core 6.0.
CVE-2019-0820	A denial-of-service vulnerability exists when the .NET Framework and .NET Core improperly process regular expression (RegEx) strings, also known as the '.NET Framework and .NET Core Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0980 and CVE-2019-0981.
CVE-2021-24112	.NET Core Remote Code Execution Vulnerability
CVE-2022-41064	.NET Framework Information Disclosure Vulnerability
CVE-2023-29331	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability
CVE-2023-46233	crypto-js is a JavaScript library of crypto standards. Prior to version 4.2.0, the crypto-js PBKDF2 algorithm was 1,000 times weaker than originally specified in 1993 and at least 1,300,000 times weaker than the current industry standard. This is because it both defaults to SHA1, a cryptographic hash algorithm considered insecure since at least 2005, and defaults to one single iteration, a 'strength' or 'difficulty' value specified at 1,000 when specified in 1993. PBKDF2 relies on iteration count as a countermeasure to preimage and collision attacks. If used to protect passwords, the impact is high. If used to generate signatures, the impact is high. Version 4.2.0 contains a patch for this issue. As a workaround, configure crypto-js to use SHA256 with at least 250,000 iterations.
CVE-2024-0056	Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vulnerability
CVE-2024-21907	Newtonsoft.Json versions before 13.0.1 are affected by a mishandling of exceptional conditions vulnerability. Crafted data that is passed to the JsonConvert.The DeserializeObject method may trigger a StackOverflow exception, resulting in a denial of service. Depending on the library's usage, an unauthenticated and remote attacker may be able to cause a denial-of-service condition.
CVE-2024-29857	An issue was discovered in ECCurve.java and ECCurve.cs in Bouncy Castle Java (BC Java) before version 1.78, BC Java LTS before version 2.73.6, BC-FJA before version 1.0.2.5, and BC C# .NET before version 2.3.1. Importing an EC certificate with crafted F2m parameters can lead to excessive CPU consumption during the evaluation of the curve parameters.
CVE-2024-30171	An issue was discovered in the Bouncy Castle Java TLS API and JSSE Provider before version 1.78. Timing-based leakage may occur in RSA-based handshakes due to exception processing.
CVE-2024-30172	An issue was discovered in the Bouncy Castle Java Cryptography APIs before 1.78. An Ed25519 verification code infinite loop can occur via a crafted signature and public key.
CVE-2024-32655	Npgsql is the .NET data provider for PostgreSQL. The `WriteBind()` method in `src/Npgsql/Internal/NpgsqlConnector.FrontendMessages.cs` uses `int` variables to store the message length and the sum of parameter lengths. Both variables overflow when the sum of parameter lengths becomes too large. This causes Npgsql to write a message size that is too small when constructing a Postgres protocol message to send it over the network to the database. When parsing the message, the database will only read a small number of bytes and treat any subsequent bytes as part of a new message, even if they belong to the old message. Attackers can abuse this to inject arbitrary Postgres protocol messages into the connection, leading to the execution of arbitrary SQL statements on the application's behalf. This vulnerability is fixed in 4.0.14, 4.1.13, 5.0.18, 6.0.11, 7.0.7, and 8.0.3.

REFERENCE NUMBER	DESCRIPTION
CVE-2024-37890	ws is an open source WebSocket client and server for Node.js. A request with a number of headers exceeding theserver.maxHeadersCount threshold could be used to crash a ws server. The vulnerability was fixed in ws@8.17.1 (e55e510) and backported to ws@7.5.10 (22c2876), ws@6.2.3 (eeb76d3), and ws@5.2.4 (4abd8f6). In vulnerable versions of ws, the issue can be mitigated in the following ways: 1. Reduce the maximum allowed length of the request headers using the --max-http-header-size=size and/or the maxHeaderSize options so that no more headers than the server.maxHeadersCount limit can be sent. 2. Set server.maxHeadersCount to 0 so that no limit is applied.
CVE-2025-25977	An issue in canvg v.4.0.2 allows an attacker to execute arbitrary code via the Constructor of the class StyleElement.

3. Version 1.4 Update Information

September 30, 2024

This version of Vertiv™ Next Connect focuses on added features, performance enhancements, platform updates, bug fixes, and security updates.

Features and Enhancements

- Cloud
  - Feature – Alarms can be cleared manually from dashboard widgets and alarm tabs.
  - Feature – Multi-Factor Authentication via Email or SMS.
  - Improvement – Added Audit Log to Users.
  - Improvement – Vertiv™ PowerIT IMD-5 support.
  - Improvement – Vertiv™ Geist™ IMD-3/Vertiv™ PowerIT IMD-5 Firmware Version 6.0.x+ support.
  - Improvement – Feedback + Suggestions form added.
  - Improvement – Performance improvements in handling of current values.
- Local Agent
  - Feature – Add Events and Alarms tabs to Local Agent.
  - Improvement – Report Agent IP Address(es) to the Cloud.
  - Improvement – Create an alarm when the local agent is offline.
  - Improvement – Suppress device alarm “noise” when the agent is offline.
- Newly Supported Devices
  - Vertiv™ Liebert® APS UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Edge 230V UPS with the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card
  - Vertiv™ Liebert® XDU1350

Bug Fixes

- Improved asset model selector and device add/edit screen.
- Improved audit logging when adding/editing/deleting objects.
- Improved redirect/authorization when logging in as an expired user.
- Improved logging of bulk firmware updates.
- Changed the messaging when trying to log in as an invalid or disabled user.
- Fixed issue where the same device could be added twice to a customer.

- Fixed issues where the sessions were not expiring or were expiring in the background.
- Fixed issues with discovering Vertiv™ Geist™ Watchdog devices via a broadcast scan.
- Fixed issue where filters were not working on the Alarms tab.
- Fixed issue where removing visibility to a group did not remove visibility to its child devices.
- Fixed issue where the MAC address is sometimes missing from the discovery scan.
- Fixed issue with the date on the configuration file list
- Fixed issue where specific alarms were not cleared.
- Fixed issue where the allocation field was not populated for customers.
- Fixed issue where the configuration card admin button would sometimes disappear.
- Removed redundant status messages when creating devices, groups, and sites.
- Added tooltips to icons in alarms/logs.
- Fixed cosmetic issues with the floorplan and map widgets.
- Fixed cosmetic issue with the numeric widget large COV indicator.
- Fixed cosmetic issues in the dashboard configuration at different resolutions.
- Added in-progress overlay for long-running operations.
- Fixed issue where some mandatory fields were not indicated.
- Fixed issue with some agents not receiving configuration updates.
- Fixed issue where local agent version information is not updated.
- Improved refresh rate and logging of agent version changes.
- Fixed issue when deleting groups in bulk.
- Fixed validation of polling rates.
- Fixed issue where the users tab was not appropriately hidden.
- Fixed issue where device fields were intermittently auto-cleared.
- Fixed cosmetic issue with the license banner.

4. Version 1.3.1 Update Information

July 2, 2024

Features and Enhancements

- Cloud
    - Feature – Save Dashboard as PDF.
    - Feature – Export Logs (Audit/Event/Alarm) to CSV.
    - Improvement – Added uniqueness check (name/address) when creating partners and customers.
    - Improvement – Upgraded Platform to .NET Core 8.
    - Improvement – Refactored event and alarm logs to improve readability.
- Local Agent
    - Improvement – Updated Agent Installer and Running Agent (Windows/Linux) to .NET Core 8.
    - Improvement – Refactored IPv6 HTTP client to use .NET 8.0 native libraries.

Bug Fixes

- Improved license enforcement and notifications.
- Improved audit logging, including updates, deletions, provisioning actions, dashboards, and linking behavior.
- Fixed issue with audit logs where org ID did not resolve to the name.

- Fixed issue where other events were hidden when the user does not have the audit log permission.
- Fixed issue with downloading one or multiple agent logs.
- Fixed issue where the device name did not change in the logs when expected.
- Fixed issue where clicking the IP address when editing a device caused problems with saving.
- Fixed issue where SNMP credentials were not saved as expected when adding a device from discovery.
- Fixed issue that occurred intermittently when provisioning SNMP v3 credentials.
- Fixed issue where the user was redirected to the home page after clicking recently added devices.
- Added the “Add for Monitoring” option to the ellipsis menu for monitored devices.
- Fixed issue where changes could be lost when adding a device for monitoring.
- Fixed issue where alarms were not cleared when a device was deleted.
- Fixed issue where alarm notifications were not grouped into single notifications.
- Fixed issue where the firmware version did not update after provisioning.
- Fixed issue where the firmware version is not displayed.
- Fixed issue where the firmware update process incorrectly reported an error for successful updates.
- Fixed issue with permissions inheritance.
- Fixed issues with initializing and adjusting visibility permissions.
- Fixed issue where groups did not load for devices.
- Fixed issue with the counts when deleting entities.
- Fixed issue with inconsistencies when accessing users.
- Fixed issue with validation when creating users.
- Fixed issue with validation on agent polling rates.
- Added cosmetic improvements:
  - Improved the sizing, buttons, and drop-down locations on mobile views.
  - Improved other buttons, widget headers, and view toggles.

Security Updates

REFERENCE NUMBER	DESCRIPTION
CVE-2024-0985	Late privilege drop in REFRESH MATERIALIZED VIEW CONCURRENTLY in PostgreSQL allows an object creator to execute arbitrary SQL functions as the command issuer. The command intends to run SQL functions as the owner of the materialized view, enabling safe refresh of untrusted materialized views. The victim is a superuser or member of one of the attacker's roles. The attack requires luring the victim into running REFRESH MATERIALIZED VIEW CONCURRENTLY on the attacker's materialized view. As part of exploiting this vulnerability, the attacker creates functions that use CREATE RULE to convert the internally built temporary table to a view. Versions before PostgreSQL 15.6, 14.11, 13.14, and 12.18 are affected. The only known exploit does not work in PostgreSQL 16 and later. For defense in depth, PostgreSQL 16.2 adds the protections that older branches are using to fix their vulnerability.
CVE-2023-32571	Dynamic Linq 1.0.7.10 through 1.2.25, before 1.3.0, allows attackers to execute arbitrary code and commands when untrusted input to methods, including Where, Select, and OrderBy, is parsed.
CVE-2023-36414	Azure Identity SDK Remote Code Execution Vulnerability.
CVE-2023-45853	MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename, comment, or extra field. **NOTE: MiniZip is not a supported part of the zlib product.**

REFERENCE NUMBER	DESCRIPTION
	NOTE: pyminizip through 0.2.6 is also vulnerable because it bundles an affected zlib version and exposes the applicable MiniZip code through its compress API.
CVE-2021-21252	The jQuery Validation Plugin provides drop-in validation for your existing forms. It is published as an npm package "jquery-validation". Prior to version 1.19.3, jquery-validation contains one or more regular expressions that are vulnerable to ReDoS (Regular Expression Denial of Service). This vulnerability issue is fixed in version 1.19.3.
CVE-2021-24112	.NET Core Remote Code Execution Vulnerability.
CVE-2021-26701	.NET Core Remote Code Execution Vulnerability.
CVE-2021-43306	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the jquery-validation npm package when an attacker is able to supply arbitrary input to the url2 method.
CWE-384	Session Fixation.
CWE-614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute.
CWE-1004	Sensitive Cookie Without 'HttpOnly' Flag.

5. Version 1.3.0 Information (Initial Release)

April 23, 2024

Version 1.3.0 is the initial release of Vertiv™ Next Connect.