CCU Release Notes

For CS-OS release r4.11.8-0-g2ac692222

CTEK Sweden AB

2026-04-24

Contents

1 Notifications

- As of 4.10.X the allowed ciphers have been reduced meaning any backend not supporting these will not work
  - Supported ciphers for TLS 1.2:
    - CDHE-ECDSA-AES256-GCM-SHA384
    - ECDHE-ECDSA-AES128-GCM-SHA256
    - ECDHE-PSK-CHACHA20-POLY1305
    - PSK-AES128-GCM-SHA256

    - ECDHE-RSA-AES256-GCM-SHA384
    - AES256-GCM-SHA384
  - Supported ciphers for TLS 1.3:
    - TLS_AES_256_GCM_SHA384
    - TLS_AES_128_GCM_SHA256
    - TLS_CHACHA20_POLY1305_SHA256

- After upgrade to 4.9.x it will not be possible to downgrade to an earlier version, this is a security improvement.
- Support for older EVSE types than Chargestorm Connected 2 has been removed, and it will not be possible to upgrade to this version.
- CGC100: need to upgrade to 3.18.X before upgrading to 4.2.X or later.

2 Version: r4.11.8

What is new?

- Web configuration interface:
  - Added Waybler as suggested backend provider
  - Added Aimo Charge as suggested backend provider
  - Added log level selector to security tab

What is changed?

- **CHARGESTORM® CONNECTED 3EI** specific:
  - Now shows uploaded screensavers and logos in the web configuration interface
  - Improved error messages when uploading screensavers and logos fail
  - Added tooltips for the custom screensaver and logo upload fields in the web configuration interface
  - UX improvements to QR code configuration, it should now be clearer how to set up QR codes and what the different fields mean
- Web configuration interface:
  - Improved localization
  - Swapped security alert pop-up for an exclamation mark in the sidebar and in the security log tab
  - Removed backend provider icons
  - Renamed "advanced charger settings" to "file management" to make it clearer what it contains

  - Added new tab "Advanced" and moved demo, MQTT and ModbusTCP settings there

What is fixed?

- **CHARGESTORM® CONNECTED 3EI** specific:
  - Fixed QR code not showing up on display unless TOTP is activated
  - Changed StationPincode to be read/write instead of write only.
- Web configuration interface:
  - Fixed RCD sensor self-test showing up on wrong charger models
  - Display settings tab will now only show up on applicable models
  - Fixed EV ready and EVSE ready being reversed

3 Version: r4.11.7

What is fixed?

- **CHARGESTORM® CONNECTED 3EI** specific:
  - Fixed a PIN code authorization issue

4 Version: r4.11.6

What is new?

- Web configuration interface:
  - Adds a password visibility toggle to the login screen
- **CHARGESTORM® CONNECTED 3EI** specific:
  - Adds support for PIN code "pre" authorization
    * A PIN code can be used in conjunction with other authorization methods, when activated, a PIN code needs to be provided before authorization through other means can start
    * Added parameters StationPinCodeEnable, StationPinCodeAllowRemoteStart, and StationPinCode

What is changed?

- **CHARGESTORM® CONNECTED 3EI** specific:
  - Added a timeout for the charging complete screen, as it previously returned to the idle screen when unplugging the car

  - Improved localization
  - Reduced unnecessary information shown on the display

- **CHARGESTORM® CONNECTED 3** specific:
  - No longer sends Ongoing in the first chargeParameterDiscoveryReq, preventing some Volvo and Polestar cars from using autocharge

What is fixed?

- Fixed an issue where power did not update in penalty mode

5 Version: r4.11.5

What is new?

- Web configuration interface:
  - Added German localization to the WebUI
  - Added Greenflux and Vialumina as suggested backend providers
  - Added modem reset button
  - Added information about the OCUs under System information
  - Added an enable debug interface toggle
- **CHARGESTORM® CONNECTED 3EI** specific:
  - Updated the information tab on the display with additional information and improved clarity
  - Added parameters for setting the customer support email and website, which are shown when the charger is in a faulty state
    - Parameters "SupportSite" and "SupportText" can be used to set these values through OCPP, these can be set during runtime
  - Added a default language parameter for the display:
    - Parameter "Language" can be used to set default language through OCPP
  - Added custom screensavers and logos
    - These can be uploaded, downloaded, and removed through the Web configuration interface
    - See datatransfers.pdf, section ResourceInstallation, for how to add them using OCPP
    - Screensavers and logos need to be in the file format .png
    - Screensavers need to be the size 800x480 px
    - Logos need to be between 10x50 px and 50x400 px in size

  - In the Faulty state, the active error code and suggested solution will be shown on the display
  - Added EichrechtSessionLimit error, which is set when the internal cached session storage is full and no additional session can be started
  - Web configuration interface:
    * Added configurations for display and Eichrecht parameters

What is changed?

- Web configuration interface:
  - Moved language selection to nav bar
  - Diagnostics page now loads into the diagnostics tab
  - Renamed "Reload configuration" to "Soft reboot"
  - Improved UX by indicating disabled outlets in grey instead of making them disappear
  - Improved visibility for option buttons
  - Improved the feedback message when downloading diagnostics
- **CHARGESTORM® CONNECTED 3EI** specific:
  - Tuned the reasons for the display and energy-meters to light up
  - Removed the requirement that QR codes need to be unique
  - Updated data-transfers RunningCost and FinalCost to use org.openchargealliance.costmsg as VendorId
  - The display will return to the default language and set dark mode when dimming down if no charge session is active
  - Updated the public key to match the "Signed Meter Values in OCPP" whitepaper
  - Always turns on the corresponding energy meter backlight during active charging sessions
  - The charger will no longer go to available before the OCMF file is sent to the backend
  - General visual improvements
  - Improved localization
  - Improved handling of errors from the energy meter
  - webPaymentStationId will default to chargeBoxIdentity if not set
  - LEDs will light solid blue when charging and during EvReady
- Removed option to allow charging on lock error for CC3 and CC3EI

What is fixed?

- Web configuration interface:
  - Fixed ep spot and chargenode showing up as one backend provider
  - Fixed the need to scroll up to see the "Unsaved changes" popup
  - Fixed backend provider being empty after first login
  - Fixed tag admin page not updating after uploading new tag
  - Fixed "unsaved changes" popup when leaving Network tab even when there are no changes
  - Fixed the firmware update failure reason not being reported, leading to endless loading
  - The actual reason will now be shown when setting a new password fails
- **CHARGESTORM® CONNECTED 3EI** specific:
  - Fixed an issue leading to invalid QR codes being shown
  - Fixed an issue where the charger could hang if communication with the energy meter was lost during session end
  - Fixed an issue where the charger would go to faulty when starting a new session before the previous session closed
  - Fixed unassigned sessions lacking OCMF data not being able to close
  - Fixed LEDs being turned off after connecting to backend
  - Fixed a casting error leading to negative current flow being shown as a very large current flow
- Uploading config files with CRLF line endings will no longer lead to undefined behavior
- Changed parameters to be configurable through OCPP without restart:
  - UtcOffset
  - WebPaymentsEnabled
  - DefaultPrice
  - Iso15118AutoChargeEnabled
- Masked sensitive information in logs regarding NgIniInstall and NgIniRetrieve
- Fixed the value "true" not being true for the parameter TamperingDetection

6 Version: r4.10.5

What is changed?

- added additional Supported ciphers for TLS 1.2:
  - ECDHE-RSA-AES256-GCM-SHA384
  - AES256-GCM-SHA384

7 Version: r4.10.4

What is new?

- Web configuration interface:
  - Added drop-down menu for selecting backend provider

What is changed?

- Web configuration interface:
  - GetConfigProfiles and setConfigProfiles endpoints have been removed
  - Removed obsolete field 'Configuration code' in the configuration tab.
  - Removed the possibility to set 'charging on lock error' for an outlet.
  - Mix of aesthetic changes
  - Updated names and contents of tabs in configuration
  - Minor translation and description updates

What is fixed?

- Parameters OutletFirstPlcModem and OutletSecondPlcModem are no longer marked as read-only

8 Version: r4.10.0

What is new?

- Web configuration interface:
  - Added the ability for users to set max and min assignment for outlets
  - Added Chargebox ID label and value to the navbar

What is changed?

- Web configuration interface:
  - Major overhaul of interface:
    - Split Wi-Fi and password settings
    - Clarified diagnostics view
    - Rephrased the title above 'Reload configuration' and 'Reboot charger' buttons
    - Clarified the uploading file process in the firmware view
    - Mix of aesthetic changes
    - Refactored the firmware view
    - Improved feedback of when a soft reset or reboot is required after configuration or firmware changes
    - Improve save awareness in Nanogrid view
    - Changed place on system and network information in the system information view
    - Removed drop-down boxes in GridUi
    - Removed platform button for non fab users
    - Total energy consumed by external meter now shown in kWh
    - Updates to tooltips and labels
    - Updated names and contents of tabs in configuration
- OCPP:
  - Parameters that do not affect the charger are now hidden from ChangeConfiguration
- Licenses have been removed
- Reduced allowed ciphers to:
  - For TLS 1.2:
    - CDHE-ECDSA-AES256-GCM-SHA384
    - ECDHE-ECDSA-AES128-GCM-SHA256
    - ECDHE-PSK-CHACHA20-POLY1305
    - PSK-AES128-GCM-SHA256
  - For TLS 1.3:
    - TLS_AES_256_GCM_SHA384
    - TLS_AES_128_GCM_SHA256
    - TLS_CHACHA20_POLY1305_SHA256

What is fixed?

- OCPP:
  - Fixed an issue where StopTransaction and MeterValues could have different values (0.1kW diff)
  - Fixed an issue where the charger could not connect to OCPP backend if no pingreboot server was specified
- Web configuration interface:
  - Fixed drop-down issue in Safari browser
  - Fixed text in the tooltips under DHCP range
  - Fixed single outlet not rendering properly
  - Fixed setting non digit value as station fuse rating
  - Fixed webUI reloads and jumps in mobile view
  - Fixed modem information does not match with the system information design
  - Fixed error messages when failed upload
  - Fixed the outlet graph boxes under system information not having the same size
  - Fixed power label not cleared when going from charging to available
  - Fixed language drop-down so it does not get cut off

Patched CVEs: see APPENDIX A.3

9 Version: r4.9.6

What is fixed?

- Fixed an issue that prevented the CGC500 from installing version 4.11 or newer

10 Version: r4.9.4

What is fixed?

- **CHARGESTORM® CONNECTED 3** specific:
  - Fixed an issue leading to units loosing their MAC-address, any units that have lost their MAC-address will have it restored when updating

11 Version: r4.9.3

What is changed?

- Outlet Controller Unit v0.2.10:

  - Updated PP limits according to newer standard.
  - Support for new RCD sensor.
  - Improved temperature handling for CC2 and CC3 series charger.
  - Improved CP state detection and transition.

What is fixed?

- Fixed broken support of older modem HL76XX

12 Version: r4.9.2

What is changed?

- OCPP:
  - Increase time between reconnection attempts if no time has been established
- Web configuration interface:
  - "System" field under system information has gotten a facelift
  - "Authentication Mode" option "Closed" has been renamed to "Locked"

What is fixed?

- Fixed rare case where the first time an EV is plugged in after a reset would not be detected
- Parameter outlet/1/fallback_current is no longer read_only
- Fixed an issue where the charger would continuously do NTP lookups if it fails to connect to a backend, This could lead to high CPU usage for chargers using a modem
- Increased time between wwan reconnection attempts, as this could lead to a death spiral where we never succeeded in the time allocated
- OCPP:
  - RemoteStartTransaction will now use correct tag when used on an "open" outlet
    - In previous versions the open tag was used instead
- Web configuration interface:
  - Fixed an issue which led to Modem information not being populated after resetting the charger
  - Fixed an issue leading to "total Energy consumed" field missing for energy meters
  - Fixed an issue for some web browsers which lead to username and password for Modem getting filled in with incorrect data

  - The color of totalenergy will now match the other fields
  - **CHARGESTORM® CONNECTED 3** specific:
    * Fixed an issue preventing WIFI from being repopulated after forgetting a network

13 Version: r4.9.1

What is new?

- Web configuration interface:
  - Added indication for WAN-connection

What is changed?

- **CHARGESTORM® CONNECTED 3** specific:
  - Added autocharge support for EVs supporting HLC but not ISO15118-2
    * In practice this will mean that most EVs supporting fast-charging will be able to use the autocharge feature
- OCPP:
  - Product serial-number will now be reported in OCPP bootNotification
    * for chargers that have a valid ProductSerialNumber, ProductSerialNumber will now be sent in the OCPP bootnotificationReq, if ProductSerialNumber is not set, the charger will respond with SystemSerialNumber

What is fixed?

- **CHARGESTORM® CONNECTED 3** specific:
  - The charger will now stay in commissioning mode and keep connected on a reset
    * Previously when resetting charger during commissioning, WiFi connection to the charger was lost and could only be reestablished by manually setting the charger in commissioning mode again
  - Fixed issue preventing autocharge from working together with NANOGRID™
  - Improved stability for charging through autocharge
- Fixed issue preventing charger going from Finishing to Preparing
- Web configuration interface:
  - Backend status will no longer be shown if no backend has been configured
  - Will no longer show MAC-address information for chargers not supporting autocharge

  - Fixed issue with a large number of decimals being shown for some meter readings

- OCPP:
  - Will no longer attempt to authorize empty tag during startup, if no previous session existed
  - Fixed incorrect handling of connection timeout present in 4.9.0
    - The issue prevented timeout from triggering leaving the charger in preparing indefinitely
  - When a soft reset was triggered during active charging the charger would wrongly send two consecutive startTransaction.rec : The charger will now correctly send one startTransaction.req

14 Version: r4.9.0

What is new?

- Web configuration interface:
  - Created a new diagnostic view with RCD sensor self test
  - Created a new tab under NANOGRID™ that is visible when using G100
    - The view shows G100 status including if it is locked and if it is possible to reset
  - Added backend connection status in header
  - Updated license page, license files are no longer used and handling of them has been removed
  - Reworked how network interfaces are presented
  - Reworked system information design

- ModbusTCP server:
  - Introduces new registers:
    - Limit control (read and write): used for controlling maximum assigned current
    - Maximum Assignment (read): used for reading maximum assignment to EV

- Added support for energy meter Carlo Gavazzi EM511

- Added parameters for setting minimum and maximum current assignment per outlet. These can be set over OCPP or through REST API and will take effect without restarting the charger
  - OutletFirstUserMinAssignment: Minimum current assignment for outlet 1 set by user

  - OutletFirstUserMaxAssignment: Maximum current assignment for outlet 1 set by user
  - OutletSecondUserMinAssignment: Minimum current assignment for outlet 2 set by user
  - OutletSecondUserMaxAssignment: Maximum current assignment for outlet 2 set by user
- Add support for NANOGRID™ AIR together with NANOGRID™ and NANOGRID™ HOME
  - this requires NANOGRID™ AIR software version 1.3.2 or newer
- **CHARGESTORM® CONNECTED 3** specific:
  - Added Autocharge support for Supported EVs: Allowing EVs that support ISO15118-2 using AC to authenticate via their MAC address

What is changed?

- Reworked assumption of phase usage. Previously if no current was drawn, an assumption was made that the connected EV was single phase, using only the primary phase. It now assumes that connected EVs use all available phases when no current is drawn
- Password reset is now only possible over Config interface
- Updated descriptions for outlet/*/authmode in parameters.pdf
- Web configuration interface:
  - Enable DHCP option was moved to Advanced Network settings
  - Removed obsolete fields for Wi-Fi settings
- **CHARGESTORM® CONNECTED 3** specific:
  - Fix ModbusTCP server and MQTT not working over Wi-Fi

What is fixed?

- Web configuration interface:
  - Fixed bug with the hamburger menu not closing after selecting a page on smartphone
  - Clearing Security status will now properly show as "OK" when clearing an already "OK" status
  - Improved tag validation when manually added through Tags page
  - Fixed changes to settings not being properly saved if charger was rebooted promptly after change
  - Fixed Tooltip got cut off by the dropdown menu bar

  - Wi-Fi menu will no longer show up on devices not supporting Wi-Fi
  - Fixed Charger hanging if setting an backend endpoint with invalid syntax
  - Fixed issue causing popup message regarding hasnanogrid internal error (sometimes occurred after bootup)
  - Reworded some error messages to make them more informative
  - Fixed issue preventing users from forgetting unconnected Wi-Fi networks
- OCPP:
  - A RemoteStartTransaction.req without the connectorId field will now be Rejected
  - A TxProfile with set transactionId is no longer allowed in a RemoteStartTransaction
  - Expiry-date now works in localAuthorizationList
  - Fixed incorrect sampled metervalue interval.
    * Measurands "Energy.Active.Export.Interval" and "Energy.Active.Import.Interval" was reported incorrectly. previously had accumulated session energy instead of the correct used energy between intervals.
  - Limited CiStringTypes data field types to 50 characters, any additional data will be truncated
  - increased delay before sending NAN values after energymeter lose communication
- Fixed: no security events where being logged when persistent storage was enabled
- Fixed time not being updated using NTP if WAN connection was not established during startup
- State E should now be properly read if set by EV
- Fixed issue where the charger could get stuck in error-state after software update
- Fixed issue where outlet configured in authentication mode: "open", would sometimes blink red when authorizing with RFID.
- **CHARGESTORM® CONNECTED 3** specific:
  - Stabilized WLAN functionality
  - Fixed commissioning hot-spot disconnecting every 3 minutes

Patched CVEs: see APPENDIX A.2

15 Version: r4.8.4

What is fixed?

- Rework reset mechanism and failsafe boot, fixing an issue where chargers would get stuck after reboot

16 Version: r4.8.2

What is new?

- The Modbus TCP server feature now supports running both "Automation" (exposing internal meter data) and NANOGRID™ limit control simultaneously.
  - Refer to the Automation Interface documentation for configuration details.

17 Version: r4.8.1

What is new?

- OCL FW 0.2.6:
  - Improved RCD self test, executes self test once every 24 Hours.

What is changed?

- OCL FW 0.2.6:
  - Improved contactor state detection.
  - Improved contactor control.
  - improved CP state detection and transition.

18 Version: r4.8.0

What is changed?

- The web configuration interface is now accessible through the modem network interface (configurable, default: disabled).
- During a firmware update, the LED user interface will indicate a faulted (Red) state when a charging session cannot be initiated.
- Log readability improvements.
- **CHARGESTORM® CONNECTED 3** specific:
  - Improve the display of available Wi-Fi network SSIDs in the web configuration interface.

What is fixed?

- Security improvements.
- Improve communication with internal energy meters:
  - This will prevent the energy meters to stall and report "stale" (repeatedly the same) values.
- **CHARGESTORM® CONNECTED 3** specific:
  - The commissioning hot-spot will no longer be disconnected when the charger is configured to connect to a Wi-Fi network.

Patched CVEs: see APPENDIX A.1

19 Version: r4.7.0

What is new?

- **CHARGESTORM® CONNECTED 3** specific:
  - **SoftAp Mode:**
    - Wireless network now supports simultaneous AP and Client modes (AP-STA). *Users can now use the unit's access point for configuration while it stays connected to the existing Wi-Fi network, making setup and adjustments more convenient.*
  - **Daisy Chaining with Dual Ethernet Ports:**
    - Added software support for daisy chaining through dual Ethernet ports on CC3.
- **Added support for Customer Export or Import Limitation Schemes to NANOGRID™:**
  - NANOGRID™ now supports setting a maximum import limit, according to EREC G100, enhancing energy management.
- **Support for Carlo Gavazzi 540:**
  - *Users can now use the Carlo Gavazzi 540 as an external meter for NANOGRID™, expanding the options for accurate energy monitoring and management.*

What is changed?

- **Log Improvements:**
  - Improved visibility and logging of errors, such as communication timeouts and authorization key handling.
- **NANOGRID™:**
  - Fuse nodes with type "aggregatedfuse" will now more quickly reduce provided current after detecting overcurrent.

What is fixed?

- Security improvements.
- Fixed an issue where the soft reset API did not wait for reset completion before returning. Previously, users encountered a timeout error when modifying settings and attempting to save and reboot. This issue is now resolved, ensuring a smoother and error-free reset process.
- Corrected an issue where the WebUI frontend displayed incorrect values for Modbus energy meters, including incorrect units. This fix ensures that users now see accurate measurements and units.
- Fixed a bug where the commissioning state caused indefinite retries when a faulty password was entered.
- Improved parsing to support pretty-printed JSON in OCPP communications. This fix ensures more reliable communication with OCPP-compatible devices, preventing potential failures in charge point operations and data exchange.

Patched CVEs:

- CVE-2023-48795
- CVE-2023-38469
- CVE-2023-38470
- CVE-2023-38471
- CVE-2023-38472
- CVE-2023-38473
- CVE-2022-48425
- CVE-2023-1194
- CVE-2023-3777
- CVE-2023-39191
- CVE-2023-4147
- CVE-2023-45898
- CVE-2023-52457
- CVE-2023-5345
- CVE-2024-0562
- CVE-2024-26588

20 Version: r4.6.4

Date of release 2024-07-16
Note: Releases r4.6.2 and r4.6.3 are not publicly available

What is fixed?

- Security improvements.

21 Version: r4.6.1

Date of release 2024-06-13
Note: this release is not publicly available

What is new?

- Initial support for CHARGESTORM® CONNECTED 3.

22 Version: r4.6.0

Date of release 2024-06-04

What is new?

- **Local Domain Accessibility via mDNS:**
  - Devices are now accessible using local domains:
    - `<hostname>.local`
    - `<product-serial>.local`
    - `<chargeboxidentity>.local`
    - `<device-model>.local`
- **Time Synchronization:**
  - Modem-connected devices can now sync time using the base station.
- **Security Enhancements:**
  - Various security improvements have been implemented.

What is changed?

- **Demo Mode:**
  - Demo mode can now be toggled via OCPP or the WebUI.
- **NANOGRID™ Optimization:**

  - Reduced mDNS network load to improve overall performance.

- **Temperature Derating:**
  - Improved temperature management by gradually lowering the current to prevent overheating.

What is fixed?

- Fixed an issue where changing the outlet configuration from the WebUI would in some cases clear the charging profiles.
- Fixed an issue that was preventing WebUI password resets.
- Fixed an issue where the charging penalty mode did not engage when the load was negative.
- Fixed an issue where the charging penalty mode was incorrectly reset.

23 Version: r4.5.1

Date of release 2024-03-27

What is fixed?

- The modem SSH access configuration parameter (interface/modem/firewall/ssh) is now applied correctly.
- Welded relay errors are now reported correctly in OCPP StatusNotifications.

24 Version: r4.5.0

Date of release 2024-03-14

What is new?

- NANOGRID™ license handling has been removed. All chargers will allow it by default.

What is changed?

- Improved modem handling and robustness
  - Dropped support for PPP-based modem connections.
  - Modem configuration parameters (wwan0/ppp0) have been simplified to a single set prefixed with 'modem'. The new parameters are called:
    * interface/modem/pin

    - interface/modem/apn
    - interface/modem/apn/username
    - interface/modem/apn/password
    - interface/modem/apn/rat
    - interface/modem/firewall/ssh

  Legacy settings will be automatically migrated upon first boot, after that they are considered deprecated and shall not be used.

What is fixed?

- Ensure that the OCPP WebSocket reconnect attempt interval gets increased with each failed attempt (up to 10 minutes).
- Fixed an issue with "validFrom" in charging profile.
- Fixed monitoring of backend connection using websocket ping.
- Fixed a number of minor issues with the WebUI.
- Fixed issue with NANOGRID™ Equal2 scheduler where it did not assign all available capacity in certain situations.
- Improvement on integration with Ferroamp EnergyHub aimed at reducing on/off oscillation.

25 Version: r4.4.3

Date of release 2024-01-16

What is fixed?

- Restore the Local proxy functionality (broken since version r4.4.0).

26 Version: r4.4.2

Date of release 2023-12-01

What is fixed?

- Fixed issue with crashing application on misconfigured NANOGRID™.

27 Version: r4.4.1

Date of release 2023-11-24

What is fixed?

- OCCP: Fixed issue with charging profile not recurring.

28 Version: r4.4.0

Date of release 2023-11-09

What is new?

- Contactor cycle count can be read out through OCPP.
- The WebUI can now be accessed remotely.
- Firewall introduced to enhance software security.
  - SSH needs to be enabled per interface.
  - WebUI needs to be enabled per interface.
- WebUI
  - Now uses the HTTPS protocol.
  - Introduced a new UI version with support for mobile devices.
- New parameter: `outlet/X/contactor_cycle_count`
- New parameter: `interface/config/firewall/ssh`
- New parameter: `interface/eth/firewall/ssh`
- New parameter: `interface/eth/firewall/webui`
- New parameter: `interface/ppp0/firewall/ssh`
- New parameter: `interface/wlan0/firewall/ssh`
- New parameter: `interface/wlan0/firewall/webui`
- New parameter: `interface/wwan0/firewall/ssh`

What is changed?

- OCPP
  - Improved OCPP handling.
  - Contactor cycle count vendor error removed
- NANOGRID™ controller overwrites station fuse rating.
- Removed the possibility of erasing device configuration in the WebUI.

What is fixed?

- Fixed broken UPS function for CGC100.
- Security improvements to the WebUI.
- Fixed an issue where the CGC500 only generated empty diagnostic files
- OCPP
  - Fixed an issue where overcurrent/penalty showed the wrong charging state in logs and OCPP StatusNotification.
  - Fixed an issue where SecurityEventNotification did not comply with the OCPP1.6 specification.
  - Fixed an issue where a newly received TxDefaultProfile did not execute if the start time had already passed.
- NANOGRID™
  - Clients will now apply the correct fallback current at system startup if the controller is unavailable.

29 Version: r4.3.2

Date of release 2023-10-04

What is fixed?

- NANOGRID™
  - NANOGRID™ clients will now apply the correct fallback current at system startup, if the NANOGRID™ controller is not available.
- WebUI:
  - Fixed issue in WebUI where configuration fields got wrong edit rules (introduced in r4.3.1).

30 Version: r4.3.1

Date of release 2023-07-07

What is new?

- New parameter: TransmitSecurityEvents (replaces TransmitAllSecurityEvents)

What is changed?

- Changed upstream fuse to an editable field instead of selector to allow higher fuse values.
- NANOGRID™ controller overwrites station fuse rating.
- Parameter TransmitAllSecurityEvents is removed.

What is fixed?

- NANOGRID™
  - Looping between SuspendedEVSE and Charging in NANOGRID™ HOME.
  - Equal2 with CGC100 / 500 will not start charging on chargers.
  - Fallback was not assigned directly after network loss.

31 Version: r4.3.0

Date of release 2023-06-22

What is new?

- Support for secure communication in NANOGRID™
- OCPP
  - Improved support for ChargingProfile
- New parameter: LogLevel. Default: info
- New parameter: NanoGridControllerSecurity
- New parameter: NanoGridClientPresharedKey

What is changed?

- EVSE does not discard cached sessions with invalid timestamp on system startup.

What is fixed?

- NANOGRID™
  - Fixed stability issues in SFB scheduler.
  - Fixed scheduling of complex sites in EQUAL2 scheduler.

32 Version: r4.2.1

Date of release 2023-06-07

What is fixed?

- Fix modem connection issue introduced in r4.2.0
- Fix viewing meter values in web gui.
- Fix issue with user interface LEDs being dark until reboot after configuration change.

33 Version: r4.2.0

Date of release 2023-05-22

What is new?

- Support for changeable password in WebUI
- Added security log functionality.
- Support for tampering detection.
- Brute force detection.
- Security log.
- OCPP
  - Support for SecurityEventNotification
- New parameter: TransmitAllSecurityEvents
- New parameter: tampering_enabled
- New parameter: platform/hwfeatures/tampering

What is changed?

- Yocto uplift to latest patch release on Dunfell 2020-04.24-dunfell(3.1.24)
- Uplift to QT: 6.2
- Restructured CS-OS for improved security.
- Disable SSH acess by default.

What is fixed?

- OCPP
  - GetDiagnostics now handles startTime and StopTime correctly.
  - Respond to TriggerMessage before taking action.
  - SendLocalList.conf fix.
  - GetCompositeSchedule: respond with not implemented

34 Version: r3.18.0

Date of release 2023-04-24

What is new?

- New parameter "UnavailableWhenTxnStartNotPossible"
- New parameter "FaultedWhenTxnStartNotPossible"
- New parameter "KeepGreenPlugLitWhenUnavailable"

What is changed?

- OCU:
  - Optimization on OCU selftest to handle noncompliant EVs
- Renaming of cgc100 to better identify model.
- OCPP 1.6:
  - Fallback to non empty string for idTag (sets idTag to:Unknown)

35 APPENDIX

APPENDIX A.1

Patched CVEs for release 4.8

CHARGESTORM® CONNECTED 2	CHARGESTORM® CONNECTED 3	CGC500
CVE-2022-38725	CVE-2022-38725	CVE-2022-38725
CVE-2022-41409	CVE-2022-41409	CVE-2022-41409
CVE-2022-48174	CVE-2022-48174	CVE-2022-48174
CVE-2023-0464	CVE-2023-0464	CVE-2023-0464
CVE-2023-0465	CVE-2023-0465	CVE-2023-0465
CVE-2023-0466	CVE-2023-0466	CVE-2023-0466
CVE-2023-23916	CVE-2023-23916	CVE-2023-23916
CVE-2023-2603	CVE-2023-2603	CVE-2023-2603
CVE-2023-2650	CVE-2023-2650	CVE-2023-2650
CVE-2023-26604	CVE-2023-26604	CVE-2023-26604
CVE-2023-27533	CVE-2023-27533	CVE-2023-27533
CVE-2023-27534	CVE-2023-27534	CVE-2023-27534
CVE-2023-27535	CVE-2023-27535	CVE-2023-27535
CVE-2023-27536	CVE-2023-27536	CVE-2023-27536
CVE-2023-27538	CVE-2023-27538	CVE-2023-27538
CVE-2023-28320	CVE-2023-28320	CVE-2023-28320
CVE-2023-28321	CVE-2023-28321	CVE-2023-28321
CVE-2023-28322	CVE-2023-28322	CVE-2023-28322
CVE-2023-28450	CVE-2023-28450	CVE-2023-28450
CVE-2023-29491	CVE-2023-29491	CVE-2023-29491
CVE-2023-29499	CVE-2023-29499	CVE-2023-29499
CVE-2023-32611	CVE-2023-32611	CVE-2023-32611
CVE-2023-32636	CVE-2023-32636	CVE-2023-32636
CVE-2023-32643	CVE-2023-32643	CVE-2023-32643
CVE-2023-32665	CVE-2023-32665	CVE-2023-32665
CVE-2023-34969	CVE-2023-34969	CVE-2023-34969
CVE-2023-3817	CVE-2023-3817	CVE-2023-3817
CVE-2023-38545	CVE-2023-38545	CVE-2023-38545
CVE-2023-38546	CVE-2023-38546	CVE-2023-38546
CVE-2023-45853	CVE-2023-45853	CVE-2023-45853
CVE-2023-46218	CVE-2023-46218	CVE-2023-46218
CVE-2023-4807	CVE-2023-4807	CVE-2023-4807
CVE-2023-4813	CVE-2023-4813	CVE-2023-4813
CVE-2023-7104	CVE-2023-7104	CVE-2023-7104
CVE-2024-0727	CVE-2024-0727	CVE-2024-0727

APPENDIX A.2

Patched CVEs for release 4.9

CHARGESTORM® CONNECTED 2	CHARGESTORM® CONNECTED 3	CGC500
CVE-2023-50387	CVE-2023-50387	CVE-2021-34431
CVE-2021-34431	CVE-2023-52426	CVE-2021-34432
CVE-2021-34432	CVE-2024-45490	CVE-2021-41039
CVE-2021-41039	CVE-2024-45491	CVE-2023-0809
CVE-2023-0809	CVE-2024-45492	CVE-2023-28366
CVE-2023-28366	CVE-2023-4156	CVE-2023-3592
CVE-2023-3592	CVE-2023-28319	CVE-2023-5632
CVE-2023-5632	CVE-2024-7264	CVE-2023-5678
CVE-2023-5678	CVE-2022-23303	CVE-2023-4156
CVE-2023-28319	CVE-2022-23304	CVE-2023-52426
CVE-2024-7264	CVE-2023-52160	CVE-2024-45490
CVE-2023-4156	CVE-2019-10207	CVE-2024-45491
CVE-2023-52426	CVE-2019-14895	CVE-2024-45492
CVE-2024-45490	CVE-2019-14896	CVE-2023-50387
CVE-2024-45491	CVE-2019-14897	CVE-2023-28319
CVE-2024-45492	CVE-2019-14901	CVE-2024-7264
CVE-2018-12327	CVE-2019-15099	CVE-2018-12327
CVE-2018-8956	CVE-2019-18660	CVE-2018-8956
CVE-2019-8936	CVE-2019-18683	CVE-2019-8936
CVE-2020-11868	CVE-2019-19050	CVE-2020-11868
CVE-2020-13817	CVE-2019-19053	CVE-2020-13817
CVE-2020-15025	CVE-2019-19064	CVE-2020-15025
CVE-2010-5321	CVE-2019-19070	CVE-2010-5321
CVE-2015-0569	CVE-2019-19071	CVE-2015-0569
CVE-2015-0570	CVE-2019-19078	CVE-2015-0570
CVE-2015-0571	CVE-2019-19241	CVE-2015-0571
CVE-2015-2877	CVE-2019-19332	CVE-2015-2877
CVE-2015-7312	CVE-2019-19338	CVE-2015-7312
CVE-2016-2853	CVE-2019-19377	CVE-2016-2853
CVE-2016-2854	CVE-2019-19447	CVE-2016-2854
CVE-2019-12456	CVE-2019-19448	CVE-2019-12456
CVE-2019-15902	CVE-2019-19462	CVE-2019-15902
CVE-2019-16089	CVE-2019-19602	CVE-2019-16089
CVE-2019-5489	CVE-2019-19767	CVE-2019-20794
CVE-2020-10774	CVE-2019-19947	CVE-2019-5489
CVE-2020-11725	CVE-2019-19965	CVE-2020-11725
CVE-2020-25220	CVE-2019-20636	CVE-2020-25220
CVE-2021-20219	CVE-2019-20794	CVE-2021-26934
CVE-2021-3773	CVE-2019-20810	CVE-2021-3773
CVE-2021-4204	CVE-2019-20812	CVE-2021-4204
CVE-2021-4439	CVE-2019-25162	CVE-2021-4439
CVE-2021-4442	CVE-2020-10690	CVE-2021-4442
CVE-2021-47193	CVE-2020-10711	CVE-2021-47193
CVE-2021-47194	CVE-2020-10757	CVE-2021-47194
CVE-2021-47198	CVE-2020-10766	CVE-2021-47198
CVE-2021-47516	CVE-2020-10767	CVE-2021-47516
CVE-2021-47518	CVE-2020-10768	CVE-2021-47518
CVE-2021-47520	CVE-2020-10781	CVE-2021-47520
CVE-2021-47521	CVE-2020-10942	CVE-2021-47521
CVE-2021-47522	CVE-2020-11494	CVE-2021-47522
CVE-2021-47541	CVE-2020-11565	CVE-2021-47541
CVE-2021-47542	CVE-2020-11608	CVE-2021-47542
CVE-2021-47550	CVE-2020-11609	CVE-2021-47550
CVE-2021-47571	CVE-2020-11668	CVE-2021-47559
CVE-2021-47576	CVE-2020-11725	CVE-2021-47571
CVE-2021-47578	CVE-2020-11884	CVE-2021-47576
CVE-2021-47583	CVE-2020-12351	CVE-2021-47578
CVE-2021-47587	CVE-2020-12352	CVE-2021-47583
CVE-2021-47589	CVE-2020-12464	CVE-2021-47587
CVE-2021-47597	CVE-2020-12465	CVE-2021-47589
CVE-2021-47599	CVE-2020-12652	CVE-2021-47597
CVE-2021-47600	CVE-2020-12653	CVE-2021-47598
CVE-2021-47602	CVE-2020-12654	CVE-2021-47599
CVE-2021-47603	CVE-2020-12655	CVE-2021-47600
CVE-2021-47606	CVE-2020-12656	CVE-2021-47602
CVE-2021-47609	CVE-2020-12657	CVE-2021-47603
CVE-2021-47610	CVE-2020-12659	CVE-2021-47606
CVE-2021-47612	CVE-2020-12768	CVE-2021-47609
CVE-2021-47619	CVE-2020-12769	CVE-2021-47610
CVE-2021-47620	CVE-2020-12770	CVE-2021-47611
CVE-2021-47622	CVE-2020-12771	CVE-2021-47612
CVE-2021-47624	CVE-2020-12826	CVE-2021-47619
CVE-2022-48655	CVE-2020-12888	CVE-2021-47620

CVE-2022-48659	CVE-2020-13143	CVE-2021-47622
CVE-2022-48670	CVE-2020-13974	CVE-2021-47624
CVE-2022-48672	CVE-2020-14314	CVE-2022-20105
CVE-2022-48687	CVE-2020-14331	CVE-2022-20106
CVE-2022-48688	CVE-2020-14351	CVE-2022-20107
CVE-2022-48732	CVE-2020-14356	CVE-2022-20108
CVE-2022-48733	CVE-2020-14381	CVE-2022-48655
CVE-2022-48734	CVE-2020-14385	CVE-2022-48659
CVE-2022-48735	CVE-2020-14386	CVE-2022-48670
CVE-2022-48740	CVE-2020-14390	CVE-2022-48672
CVE-2022-48741	CVE-2020-14416	CVE-2022-48687
CVE-2022-48742	CVE-2020-15393	CVE-2022-48688
CVE-2022-48743	CVE-2020-15436	CVE-2022-48693
CVE-2022-48756	CVE-2020-15437	CVE-2022-48732
CVE-2022-48772	CVE-2020-15780	CVE-2022-48733
CVE-2022-48773	CVE-2020-16120	CVE-2022-48734
CVE-2022-48788	CVE-2020-16166	CVE-2022-48735
CVE-2022-48789	CVE-2020-24394	CVE-2022-48740
CVE-2022-48790	CVE-2020-24586	CVE-2022-48741
CVE-2022-48791	CVE-2020-24587	CVE-2022-48742
CVE-2022-48792	CVE-2020-24588	CVE-2022-48743
CVE-2022-48796	CVE-2020-25211	CVE-2022-48756
CVE-2022-48804	CVE-2020-25212	CVE-2022-48772
CVE-2022-48809	CVE-2020-25284	CVE-2022-48773
CVE-2022-48822	CVE-2020-25285	CVE-2022-48775
CVE-2022-48824	CVE-2020-25639	CVE-2022-48788
CVE-2022-48826	CVE-2020-25641	CVE-2022-48789
CVE-2022-48836	CVE-2020-25643	CVE-2022-48790
CVE-2022-48838	CVE-2020-25645	CVE-2022-48791
CVE-2022-48839	CVE-2020-25656	CVE-2022-48792
CVE-2022-48842	CVE-2020-25668	CVE-2022-48796
CVE-2022-48843	CVE-2020-25669	CVE-2022-48804
CVE-2022-48844	CVE-2020-25670	CVE-2022-48809
CVE-2022-48845	CVE-2020-25671	CVE-2022-48822
CVE-2022-48849	CVE-2020-25704	CVE-2022-48824
CVE-2022-48850	CVE-2020-25705	CVE-2022-48826
CVE-2022-48851	CVE-2020-26088	CVE-2022-48836
CVE-2022-48852	CVE-2020-26147	CVE-2022-48838
CVE-2022-48853	CVE-2020-26541	CVE-2022-48839
CVE-2022-48855	CVE-2020-26558	CVE-2022-48842
CVE-2022-48857	CVE-2020-27152	CVE-2022-48843
CVE-2022-48858	CVE-2020-27170	CVE-2022-48844
CVE-2022-48860	CVE-2020-27171	CVE-2022-48845
CVE-2022-48863	CVE-2020-27194	CVE-2022-48849
CVE-2022-48865	CVE-2020-27673	CVE-2022-48850
CVE-2022-48875	CVE-2020-27675	CVE-2022-48851
CVE-2022-48877	CVE-2020-27777	CVE-2022-48852
CVE-2022-48891	CVE-2020-27784	CVE-2022-48853
CVE-2022-48899	CVE-2020-27786	CVE-2022-48855
CVE-2022-48901	CVE-2020-27830	CVE-2022-48856
CVE-2022-48902	CVE-2020-28097	CVE-2022-48857
CVE-2022-48908	CVE-2020-28374	CVE-2022-48858
CVE-2022-48910	CVE-2020-28915	CVE-2022-48860
CVE-2022-48911	CVE-2020-28941	CVE-2022-48863
CVE-2022-48912	CVE-2020-28974	CVE-2022-48865
CVE-2022-48919	CVE-2020-29368	CVE-2022-48875
CVE-2022-48920	CVE-2020-29369	CVE-2022-48877
CVE-2022-48923	CVE-2020-29370	CVE-2022-48891
CVE-2022-48924	CVE-2020-29371	CVE-2022-48899
CVE-2022-48926	CVE-2020-29372	CVE-2022-48901
CVE-2022-48928	CVE-2020-29374	CVE-2022-48902
CVE-2022-48930	CVE-2020-29534	CVE-2022-48905
CVE-2022-48931	CVE-2020-29569	CVE-2022-48908
CVE-2022-48935	CVE-2020-29660	CVE-2022-48910
CVE-2022-48938	CVE-2020-29661	CVE-2022-48911
CVE-2022-48941	CVE-2020-35508	CVE-2022-48912
CVE-2022-48943	CVE-2020-35519	CVE-2022-48919
CVE-2022-48946	CVE-2020-36158	CVE-2022-48920
CVE-2022-48947	CVE-2020-36310	CVE-2022-48923
CVE-2022-48948	CVE-2020-36311	CVE-2022-48924
CVE-2022-48949	CVE-2020-36312	CVE-2022-48926
CVE-2022-48950	CVE-2020-36313	CVE-2022-48928
CVE-2022-48951	CVE-2020-36322	CVE-2022-48930
CVE-2022-48953	CVE-2020-36385	CVE-2022-48931
CVE-2022-48956	CVE-2020-36386	CVE-2022-48935
CVE-2022-48958	CVE-2020-36516	CVE-2022-48938
CVE-2022-48960	CVE-2020-36557	CVE-2022-48941
CVE-2022-48961	CVE-2020-36558	CVE-2022-48943
CVE-2022-48962	CVE-2020-36691	CVE-2022-48946

CVE-2022-48966	CVE-2020-36694	CVE-2022-48947
CVE-2022-48967	CVE-2020-36766	CVE-2022-48948
CVE-2022-48969	CVE-2020-36775	CVE-2022-48949
CVE-2022-48971	CVE-2020-36777	CVE-2022-48950
CVE-2022-48972	CVE-2020-8428	CVE-2022-48951
CVE-2022-48973	CVE-2020-8647	CVE-2022-48953
CVE-2022-48975	CVE-2020-8648	CVE-2022-48956
CVE-2022-48978	CVE-2020-8649	CVE-2022-48958
CVE-2022-48982	CVE-2020-8992	CVE-2022-48960
CVE-2022-48988	CVE-2020-9383	CVE-2022-48961
CVE-2022-48991	CVE-2020-9391	CVE-2022-48962
CVE-2022-48992	CVE-2021-20177	CVE-2022-48966
CVE-2022-48994	CVE-2021-20239	CVE-2022-48967
CVE-2022-49002	CVE-2021-20268	CVE-2022-48969
CVE-2022-49006	CVE-2021-20292	CVE-2022-48971
CVE-2022-49007	CVE-2021-20317	CVE-2022-48972
CVE-2022-49010	CVE-2021-20320	CVE-2022-48973
CVE-2022-49011	CVE-2021-20321	CVE-2022-48975
CVE-2022-49015	CVE-2021-20322	CVE-2022-48978
CVE-2022-49020	CVE-2021-22555	CVE-2022-48982
CVE-2022-49021	CVE-2021-23133	CVE-2022-48988
CVE-2022-49026	CVE-2021-23134	CVE-2022-48991
CVE-2022-49027	CVE-2021-26930	CVE-2022-48992
CVE-2022-49028	CVE-2021-26931	CVE-2022-48994
CVE-2022-49029	CVE-2021-26932	CVE-2022-49002
CVE-2022-49031	CVE-2021-26934	CVE-2022-49006
CVE-2022-49032	CVE-2021-27363	CVE-2022-49007
CVE-2022-49033	CVE-2021-27364	CVE-2022-49010
CVE-2023-1476	CVE-2021-27365	CVE-2022-49011
CVE-2023-3022	CVE-2021-28038	CVE-2022-49013
CVE-2023-52753	CVE-2021-28375	CVE-2022-49014
CVE-2023-52806	CVE-2021-28660	CVE-2022-49015
CVE-2023-52809	CVE-2021-28688	CVE-2022-49019
CVE-2023-52814	CVE-2021-28714	CVE-2022-49020
CVE-2023-52815	CVE-2021-28715	CVE-2022-49021
CVE-2023-52817	CVE-2021-28950	CVE-2022-49026
CVE-2023-52821	CVE-2021-28951	CVE-2022-49027
CVE-2023-52885	CVE-2021-28952	CVE-2022-49028
CVE-2023-52893	CVE-2021-28964	CVE-2022-49029
CVE-2023-52894	CVE-2021-28971	CVE-2022-49031
CVE-2023-52898	CVE-2021-28972	CVE-2022-49032
CVE-2023-52899	CVE-2021-29154	CVE-2022-49033
CVE-2023-52900	CVE-2021-29155	CVE-2023-1476
CVE-2023-52901	CVE-2021-29264	CVE-2023-20659
CVE-2023-52903	CVE-2021-29265	CVE-2023-20660
CVE-2023-52907	CVE-2021-29646	CVE-2023-20661
CVE-2023-52915	CVE-2021-29647	CVE-2023-20662
CVE-2023-52918	CVE-2021-29648	CVE-2023-20663
CVE-2023-52919	CVE-2021-29649	CVE-2023-20674
CVE-2024-0564	CVE-2021-29650	CVE-2023-20675
CVE-2024-26882	CVE-2021-30002	CVE-2023-20676
CVE-2024-26883	CVE-2021-30178	CVE-2023-20677
CVE-2024-26884	CVE-2021-3178	CVE-2023-20679
CVE-2024-26898	CVE-2021-31829	CVE-2023-20682
CVE-2024-26901	CVE-2021-31916	CVE-2023-20712
CVE-2024-26903	CVE-2021-32078	CVE-2023-20715
CVE-2024-26907	CVE-2021-32399	CVE-2023-20716
CVE-2024-26910	CVE-2021-33033	CVE-2023-20810
CVE-2024-26929	CVE-2021-33034	CVE-2023-20811
CVE-2024-26934	CVE-2021-3347	CVE-2023-20838
CVE-2024-27013	CVE-2021-3348	CVE-2023-3022
CVE-2024-27018	CVE-2021-33624	CVE-2023-32810
CVE-2024-27019	CVE-2021-33656	CVE-2023-32820
CVE-2024-27020	CVE-2021-33909	CVE-2023-52753
CVE-2024-35978	CVE-2021-3411	CVE-2023-52806
CVE-2024-35982	CVE-2021-3428	CVE-2023-52809
CVE-2024-35984	CVE-2021-3444	CVE-2023-52814
CVE-2024-35997	CVE-2021-34556	CVE-2023-52815
CVE-2024-36270	CVE-2021-34693	CVE-2023-52817
CVE-2024-36897	CVE-2021-3483	CVE-2023-52821
CVE-2024-36969	CVE-2021-3501	CVE-2023-52885
CVE-2024-36971	CVE-2021-35039	CVE-2023-52893
CVE-2024-38546	CVE-2021-3506	CVE-2023-52894
CVE-2024-38547	CVE-2021-35477	CVE-2023-52898
CVE-2024-38549	CVE-2021-3573	CVE-2023-52899
CVE-2024-38583	CVE-2021-3600	CVE-2023-52900
CVE-2024-38597	CVE-2021-3609	CVE-2023-52901
CVE-2024-38600	CVE-2021-3612	CVE-2023-52903
CVE-2024-38627	CVE-2021-3635	CVE-2023-52907

CVE-2024-38633	CVE-2021-3640	CVE-2023-52915
CVE-2024-38661	CVE-2021-3653	CVE-2023-52918
CVE-2024-38667	CVE-2021-3655	CVE-2023-52919
CVE-2024-39277	CVE-2021-3656	CVE-2024-0564
CVE-2024-39301	CVE-2021-3659	CVE-2024-26882
CVE-2024-39468	CVE-2021-3679	CVE-2024-26883
CVE-2024-39471	CVE-2021-3715	CVE-2024-26884
CVE-2024-39487	CVE-2021-37159	CVE-2024-26898
CVE-2024-39489	CVE-2021-3732	CVE-2024-26901
CVE-2024-39495	CVE-2021-3736	CVE-2024-26903
CVE-2024-40902	CVE-2021-3739	CVE-2024-26907
CVE-2024-40904	CVE-2021-3744	CVE-2024-26910
CVE-2024-40905	CVE-2021-3752	CVE-2024-26929
CVE-2024-40911	CVE-2021-3753	CVE-2024-26934
CVE-2024-40912	CVE-2021-37576	CVE-2024-27013
CVE-2024-40932	CVE-2021-3760	CVE-2024-27018
CVE-2024-40959	CVE-2021-3764	CVE-2024-27019
CVE-2024-40960	CVE-2021-3772	CVE-2024-27020
CVE-2024-40967	CVE-2021-3773	CVE-2024-35978
CVE-2024-40970	CVE-2021-38160	CVE-2024-35982
CVE-2024-40980	CVE-2021-38166	CVE-2024-35984
CVE-2024-40981	CVE-2021-38198	CVE-2024-35997
CVE-2024-41000	CVE-2021-38199	CVE-2024-36270
CVE-2024-41002	CVE-2021-38200	CVE-2024-36897
CVE-2024-41012	CVE-2021-38202	CVE-2024-36969
CVE-2024-41046	CVE-2021-38203	CVE-2024-36971
CVE-2024-41059	CVE-2021-38204	CVE-2024-38546
CVE-2024-41060	CVE-2021-38205	CVE-2024-38547
CVE-2024-41063	CVE-2021-38206	CVE-2024-38549
CVE-2024-41064	CVE-2021-38207	CVE-2024-38552
CVE-2024-41070	CVE-2021-38208	CVE-2024-38583
CVE-2024-41073	CVE-2021-38209	CVE-2024-38597
CVE-2024-41089	CVE-2021-38300	CVE-2024-38600
CVE-2024-41093	CVE-2021-3923	CVE-2024-38627
CVE-2024-41095	CVE-2021-4001	CVE-2024-38633
CVE-2024-41097	CVE-2021-4023	CVE-2024-38661
CVE-2024-42068	CVE-2021-4032	CVE-2024-38667
CVE-2024-42070	CVE-2021-4037	CVE-2024-38780
CVE-2024-42076	CVE-2021-40490	CVE-2024-39277
CVE-2024-42077	CVE-2021-4083	CVE-2024-39292
CVE-2024-42080	CVE-2021-4148	CVE-2024-39301
CVE-2024-42082	CVE-2021-4149	CVE-2024-39468
CVE-2024-42090	CVE-2021-4150	CVE-2024-39471
CVE-2024-42093	CVE-2021-4154	CVE-2024-39475
CVE-2024-42094	CVE-2021-4157	CVE-2024-39476
CVE-2024-42101	CVE-2021-4159	CVE-2024-39480
CVE-2024-42104	CVE-2021-41864	CVE-2024-39487
CVE-2024-42131	CVE-2021-42008	CVE-2024-39489
CVE-2024-42148	CVE-2021-4203	CVE-2024-39495
CVE-2024-42152	CVE-2021-4204	CVE-2024-39506
CVE-2024-42153	CVE-2021-42252	CVE-2024-40902
CVE-2024-42154	CVE-2021-42327	CVE-2024-40904
CVE-2024-42157	CVE-2021-42739	CVE-2024-40905
CVE-2024-42161	CVE-2021-43056	CVE-2024-40911
CVE-2024-42223	CVE-2021-43389	CVE-2024-40912
CVE-2024-42224	CVE-2021-43975	CVE-2024-40932
CVE-2024-42225	CVE-2021-43976	CVE-2024-40959
CVE-2024-42229	CVE-2021-4439	CVE-2024-40960
CVE-2024-42232	CVE-2021-4441	CVE-2024-40961
CVE-2024-42236	CVE-2021-4442	CVE-2024-40967
CVE-2024-42244	CVE-2021-44733	CVE-2024-40970
CVE-2024-42259	CVE-2021-45095	CVE-2024-40980
CVE-2024-42271	CVE-2021-45469	CVE-2024-40981
CVE-2024-42280	CVE-2021-45480	CVE-2024-40995
CVE-2024-42284	CVE-2021-45485	CVE-2024-41000
CVE-2024-42285	CVE-2021-45486	CVE-2024-41002
CVE-2024-42286	CVE-2021-45868	CVE-2024-41007
CVE-2024-42288	CVE-2021-46283	CVE-2024-41012
CVE-2024-42289	CVE-2021-46904	CVE-2024-41046
CVE-2024-42301	CVE-2021-46905	CVE-2024-41059
CVE-2024-42302	CVE-2021-46906	CVE-2024-41060
CVE-2024-42309	CVE-2021-46909	CVE-2024-41063
CVE-2024-42310	CVE-2021-46915	CVE-2024-41064
CVE-2024-42311	CVE-2021-46921	CVE-2024-41070
CVE-2024-42313	CVE-2021-46924	CVE-2024-41073
CVE-2024-43854	CVE-2021-46925	CVE-2024-41087
CVE-2024-43856	CVE-2021-46926	CVE-2024-41089
CVE-2024-43858	CVE-2021-46928	CVE-2024-41093
CVE-2024-43860	CVE-2021-46929	CVE-2024-41095

CVE-2024-43861	CVE-2021-46930	CVE-2024-41097
CVE-2024-43863	CVE-2021-46932	CVE-2024-42068
CVE-2024-43871	CVE-2021-46933	CVE-2024-42070
CVE-2024-43882	CVE-2021-46934	CVE-2024-42076
CVE-2024-43890	CVE-2021-46935	CVE-2024-42077
CVE-2024-43893	CVE-2021-46936	CVE-2024-42080
CVE-2024-43902	CVE-2021-46938	CVE-2024-42082
CVE-2024-43903	CVE-2021-46939	CVE-2024-42090
CVE-2024-43907	CVE-2021-46941	CVE-2024-42093
CVE-2024-43908	CVE-2021-46943	CVE-2024-42094
CVE-2024-43909	CVE-2021-46944	CVE-2024-42101
CVE-2024-43914	CVE-2021-46950	CVE-2024-42104
CVE-2024-44947	CVE-2021-46951	CVE-2024-42114
CVE-2024-44954	CVE-2021-46953	CVE-2024-42131
CVE-2024-44960	CVE-2021-47171	CVE-2024-42148
CVE-2024-44969	CVE-2021-47173	CVE-2024-42152
CVE-2024-44987	CVE-2021-47193	CVE-2024-42153
CVE-2024-44998	CVE-2021-47194	CVE-2024-42154
CVE-2024-44999	CVE-2021-47198	CVE-2024-42157
CVE-2024-45003	CVE-2021-47516	CVE-2024-42161
CVE-2024-45021	CVE-2021-47518	CVE-2024-42223
CVE-2024-45025	CVE-2021-47520	CVE-2024-42224
CVE-2024-45028	CVE-2021-47521	CVE-2024-42225
CVE-2024-46673	CVE-2021-47522	CVE-2024-42229
CVE-2024-46674	CVE-2021-47541	CVE-2024-42232
CVE-2024-46675	CVE-2021-47542	CVE-2024-42236
CVE-2024-46676	CVE-2021-47546	CVE-2024-42244
CVE-2024-46677	CVE-2021-47550	CVE-2024-42259
CVE-2024-46679	CVE-2021-47559	CVE-2024-42271
CVE-2024-46685	CVE-2021-47571	CVE-2024-42280
CVE-2024-46702	CVE-2021-47572	CVE-2024-42284
CVE-2024-46707	CVE-2021-47576	CVE-2024-42285
CVE-2024-46756	CVE-2021-47578	CVE-2024-42286
CVE-2024-46757	CVE-2021-47583	CVE-2024-42288
CVE-2024-46758	CVE-2021-47587	CVE-2024-42289
CVE-2024-49967	CVE-2021-47589	CVE-2024-42301
CVE-2024-50018	CVE-2021-47597	CVE-2024-42302
CVE-2024-50089	CVE-2021-47598	CVE-2024-42309
	CVE-2021-47599	CVE-2024-42310
	CVE-2021-47600	CVE-2024-42311
	CVE-2021-47602	CVE-2024-42313
	CVE-2021-47603	CVE-2024-43854
	CVE-2021-47606	CVE-2024-43856
	CVE-2021-47609	CVE-2024-43858
	CVE-2021-47610	CVE-2024-43860
	CVE-2021-47611	CVE-2024-43861
	CVE-2021-47612	CVE-2024-43863
	CVE-2021-47619	CVE-2024-43871
	CVE-2021-47620	CVE-2024-43882
	CVE-2021-47622	CVE-2024-43890
	CVE-2021-47624	CVE-2024-43893
	CVE-2022-0322	CVE-2024-43902
	CVE-2022-0480	CVE-2024-43903
	CVE-2022-0487	CVE-2024-43907
	CVE-2022-0812	CVE-2024-43908
	CVE-2022-0850	CVE-2024-43909
	CVE-2022-1158	CVE-2024-43914
	CVE-2022-1419	CVE-2024-44947
	CVE-2022-1508	CVE-2024-44954
	CVE-2022-1652	CVE-2024-44960
	CVE-2022-1679	CVE-2024-44965
	CVE-2022-1729	CVE-2024-44969
	CVE-2022-1789	CVE-2024-44982
	CVE-2022-25636	CVE-2024-44987
	CVE-2022-2588	CVE-2024-44995
	CVE-2022-26365	CVE-2024-44998
	CVE-2022-2639	CVE-2024-44999
	CVE-2022-2938	CVE-2024-45003
	CVE-2022-29581	CVE-2024-45006
	CVE-2022-2964	CVE-2024-45021
	CVE-2022-2977	CVE-2024-45025
	CVE-2022-2991	CVE-2024-45028
	CVE-2022-3028	CVE-2024-46673
	CVE-2022-30594	CVE-2024-46674
	CVE-2022-3176	CVE-2024-46675
	CVE-2022-3202	CVE-2024-46676
	CVE-2022-32250	CVE-2024-46677
	CVE-2022-3239	CVE-2024-46679
	CVE-2022-33740	CVE-2024-46685

	CVE-2022-33741	CVE-2024-46689
	CVE-2022-33742	CVE-2024-46702
	CVE-2022-34918	CVE-2024-46707
	CVE-2022-3577	CVE-2024-46756
	CVE-2022-3625	CVE-2024-46757
	CVE-2022-36280	CVE-2024-46758
	CVE-2022-3635	CVE-2024-49967
	CVE-2022-36946	CVE-2024-50018
	CVE-2022-39189	CVE-2024-50089
	CVE-2022-40476	
	CVE-2022-4095	
	CVE-2022-41222	
	CVE-2022-41858	
	CVE-2022-48626	
	CVE-2022-48654	
	CVE-2022-48655	
	CVE-2022-48659	
	CVE-2022-48670	
	CVE-2022-48672	
	CVE-2022-48674	
	CVE-2022-48686	
	CVE-2022-48687	
	CVE-2022-48688	
	CVE-2022-48693	
	CVE-2022-48732	
	CVE-2022-48733	
	CVE-2022-48734	
	CVE-2022-48735	
	CVE-2022-48740	
	CVE-2022-48741	
	CVE-2022-48742	
	CVE-2022-48743	
	CVE-2022-48756	
	CVE-2022-48773	
	CVE-2022-48775	
	CVE-2022-48788	
	CVE-2022-48789	
	CVE-2022-48790	
	CVE-2022-48791	
	CVE-2022-48792	
	CVE-2022-48796	
	CVE-2022-48804	
	CVE-2022-48809	
	CVE-2022-48822	
	CVE-2022-48824	
	CVE-2022-48826	
	CVE-2022-48836	
	CVE-2022-48838	
	CVE-2022-48839	
	CVE-2022-48842	
	CVE-2022-48843	
	CVE-2022-48844	
	CVE-2022-48845	
	CVE-2022-48849	
	CVE-2022-48850	
	CVE-2022-48851	
	CVE-2022-48852	
	CVE-2022-48853	
	CVE-2022-48855	
	CVE-2022-48856	
	CVE-2022-48857	
	CVE-2022-48858	
	CVE-2022-48860	
	CVE-2022-48863	
	CVE-2022-48865	
	CVE-2022-48901	
	CVE-2022-48902	
	CVE-2022-48905	
	CVE-2022-48908	
	CVE-2022-48909	
	CVE-2022-48910	
	CVE-2022-48911	
	CVE-2022-48912	
	CVE-2022-48919	
	CVE-2022-48920	
	CVE-2022-48923	
	CVE-2022-48924	
	CVE-2022-48926	
	CVE-2022-48928	

	CVE-2022-48930	
	CVE-2022-48931	
	CVE-2022-48933	
	CVE-2022-48934	
	CVE-2022-48935	
	CVE-2022-48938	
	CVE-2022-48941	
	CVE-2022-48943	
	CVE-2023-0240	
	CVE-2023-1390	
	CVE-2023-1476	
	CVE-2023-1582	
	CVE-2023-1838	
	CVE-2023-23006	
	CVE-2023-28772	
	CVE-2023-3111	
	CVE-2023-34324	
	CVE-2023-4387	
	CVE-2023-4732	
	CVE-2023-5158	
	CVE-2024-0564	
	CVE-2024-23196	
	CVE-2024-24860	
	CVE-2024-26929	
	CVE-2024-38667	
	CVE-2024-43903	
	CVE-2024-46756	
	CVE-2024-46757	
	CVE-2024-46758	
	CVE-2024-49967	
	CVE-2024-50018	
	CVE-2024-50089	
	CVE-2021-34431	
	CVE-2021-34432	
	CVE-2021-41039	
	CVE-2023-0809	
	CVE-2023-28366	
	CVE-2023-3592	
	CVE-2023-5632	
	CVE-2023-5678	

APPENDIX A.3

Patched CVEs for release 4.10.4

CHARGESTORM® CONNECTED 2	CHARGESTORM® CONNECTED 3
CVE-2024-10525	CVE-2024-52533
CVE-2024-3935	CVE-2023-34410
CVE-2024-8376	CVE-2023-37369
CVE-2024-11053	CVE-2023-38197
CVE-2024-9681	CVE-2023-43114
CVE-2025-0167	CVE-2023-51714
CVE-2023-34410	CVE-2024-25580
CVE-2023-37369	CVE-2024-36048
CVE-2023-38197	CVE-2024-39936
CVE-2023-43114	CVE-2025-30348
CVE-2023-51714	CVE-2025-57052
CVE-2024-25580	CVE-2014-2524
CVE-2024-36048	CVE-2025-6965
CVE-2024-39936	CVE-2022-2196
CVE-2025-30348	CVE-2022-2978
CVE-2025-6965	CVE-2022-3424
CVE-2014-6271	CVE-2022-3545
CVE-2014-7169	CVE-2022-3564
CVE-2016-7543	CVE-2022-3565
CVE-2016-9401	CVE-2022-3623
CVE-2019-18276	CVE-2022-3640
CVE-2019-9924	CVE-2022-3643
CVE-2022-48695	CVE-2022-3649
CVE-2022-49063	CVE-2022-4139
CVE-2022-49168	CVE-2022-41674
CVE-2022-49535	CVE-2022-42719
CVE-2023-52530	CVE-2022-42720
CVE-2023-52572	CVE-2022-42896
CVE-2023-52621	CVE-2022-43750
CVE-2023-52752	CVE-2022-4378
CVE-2023-52757	CVE-2022-4379
CVE-2023-52812	CVE-2022-45886
CVE-2023-52927	CVE-2022-45919
CVE-2023-52979	CVE-2022-45934
CVE-2024-26739	CVE-2022-47518
CVE-2024-26914	CVE-2022-47519
CVE-2024-26921	CVE-2022-47520
CVE-2024-26928	CVE-2022-47521
CVE-2024-26944	CVE-2022-47940
CVE-2024-26952	CVE-2022-48424
CVE-2024-27072	CVE-2022-48425
CVE-2024-27402	CVE-2022-48502
CVE-2024-35866	CVE-2022-48638
CVE-2024-35867	CVE-2022-48662
CVE-2024-35869	CVE-2022-48695
CVE-2024-36476	CVE-2022-48708
CVE-2024-36912	CVE-2022-48772
CVE-2024-36913	CVE-2022-48808
CVE-2024-36923	CVE-2022-48868
CVE-2024-38541	CVE-2022-48869
CVE-2024-38545	CVE-2022-48870
CVE-2024-38577	CVE-2022-48871
CVE-2024-38588	CVE-2022-48872
CVE-2024-39463	CVE-2022-48873
CVE-2024-39494	CVE-2022-48875
CVE-2024-39497	CVE-2022-48877
CVE-2024-40953	CVE-2022-48878
CVE-2024-41061	CVE-2022-48879
CVE-2024-43098	CVE-2022-48891
CVE-2024-43895	CVE-2022-48892
CVE-2024-44972	CVE-2022-48896
CVE-2024-45009	CVE-2022-48898
CVE-2024-45828	CVE-2022-48899
CVE-2024-46714	CVE-2022-48946
CVE-2024-46719	CVE-2022-48947
CVE-2024-46721	CVE-2022-48948
CVE-2024-46722	CVE-2022-48949
CVE-2024-46723	CVE-2022-48950
CVE-2024-46724	CVE-2022-48951
CVE-2024-46725	CVE-2022-48952
CVE-2024-46731	CVE-2022-48953
CVE-2024-46732	CVE-2022-48954
CVE-2024-46734	CVE-2022-48955

CVE-2024-46737	CVE-2022-48956
CVE-2024-46738	CVE-2022-48957
CVE-2024-46739	CVE-2022-48958
CVE-2024-46740	CVE-2022-48959
CVE-2024-46743	CVE-2022-48960
CVE-2024-46744	CVE-2022-48961
CVE-2024-46746	CVE-2022-48962
CVE-2024-46747	CVE-2022-48965
CVE-2024-46750	CVE-2022-48966
CVE-2024-46755	CVE-2022-48967
CVE-2024-46759	CVE-2022-48968
CVE-2024-46761	CVE-2022-48969
CVE-2024-46763	CVE-2022-48970
CVE-2024-46771	CVE-2022-48971
CVE-2024-46777	CVE-2022-48972
CVE-2024-46780	CVE-2022-48973
CVE-2024-46781	CVE-2022-48975
CVE-2024-46782	CVE-2022-48977
CVE-2024-46783	CVE-2022-48978
CVE-2024-46791	CVE-2022-48980
CVE-2024-46795	CVE-2022-48981
CVE-2024-46798	CVE-2022-48982
CVE-2024-46800	CVE-2022-48983
CVE-2024-46804	CVE-2022-48985
CVE-2024-46805	CVE-2022-48986
CVE-2024-46807	CVE-2022-48988
CVE-2024-46810	CVE-2022-48991
CVE-2024-46814	CVE-2022-48992
CVE-2024-46815	CVE-2022-48994
CVE-2024-46817	CVE-2022-48995
CVE-2024-46818	CVE-2022-48997
CVE-2024-46819	CVE-2022-48999
CVE-2024-46822	CVE-2022-49000
CVE-2024-46828	CVE-2022-49001
CVE-2024-46829	CVE-2022-49002
CVE-2024-46832	CVE-2022-49003
CVE-2024-46840	CVE-2022-49004
CVE-2024-46844	CVE-2022-49005
CVE-2024-47143	CVE-2022-49006
CVE-2024-47659	CVE-2022-49007
CVE-2024-47660	CVE-2022-49010
CVE-2024-47663	CVE-2022-49011
CVE-2024-47665	CVE-2022-49013
CVE-2024-47667	CVE-2022-49014
CVE-2024-47668	CVE-2022-49015
CVE-2024-47669	CVE-2022-49016
CVE-2024-47672	CVE-2022-49017
CVE-2024-47674	CVE-2022-49019
CVE-2024-47679	CVE-2022-49020
CVE-2024-47684	CVE-2022-49021
CVE-2024-47685	CVE-2022-49022
CVE-2024-47690	CVE-2022-49023
CVE-2024-47692	CVE-2022-49024
CVE-2024-47693	CVE-2022-49025
CVE-2024-47695	CVE-2022-49026
CVE-2024-47696	CVE-2022-49027
CVE-2024-47697	CVE-2022-49028
CVE-2024-47698	CVE-2022-49029
CVE-2024-47699	CVE-2022-49030
CVE-2024-47701	CVE-2022-49031
CVE-2024-47705	CVE-2022-49032
CVE-2024-47706	CVE-2022-49033
CVE-2024-47710	CVE-2022-49035
CVE-2024-47712	CVE-2022-49063
CVE-2024-47713	CVE-2022-49139
CVE-2024-47718	CVE-2022-49168
CVE-2024-47720	CVE-2022-49535
CVE-2024-47723	CVE-2022-49738
CVE-2024-47734	CVE-2022-49740
CVE-2024-47735	CVE-2022-49741
CVE-2024-47737	CVE-2022-49746
CVE-2024-47739	CVE-2022-49748
CVE-2024-47742	CVE-2022-49749
CVE-2024-47747	CVE-2022-49751
CVE-2024-47748	CVE-2022-49752
CVE-2024-47749	CVE-2022-49753
CVE-2024-47757	CVE-2022-49755
CVE-2024-48881	CVE-2022-49757
CVE-2024-49851	CVE-2022-49758

CVE-2024-49852	CVE-2022-49761
CVE-2024-49854	CVE-2022-49837
CVE-2024-49856	CVE-2022-49839
CVE-2024-49858	CVE-2022-49840
CVE-2024-49860	CVE-2022-49842
CVE-2024-49863	CVE-2022-49845
CVE-2024-49866	CVE-2022-49846
CVE-2024-49867	CVE-2022-49850
CVE-2024-49868	CVE-2022-49853
CVE-2024-49871	CVE-2022-49854
CVE-2024-49875	CVE-2022-49855
CVE-2024-49877	CVE-2022-49857
CVE-2024-49878	CVE-2022-49860
CVE-2024-49879	CVE-2022-49861
CVE-2024-49881	CVE-2022-49862
CVE-2024-49882	CVE-2022-49863
CVE-2024-49883	CVE-2022-49864
CVE-2024-49884	CVE-2022-49866
CVE-2024-49886	CVE-2022-49867
CVE-2024-49889	CVE-2022-49869
CVE-2024-49890	CVE-2022-49871
CVE-2024-49892	CVE-2022-49873
CVE-2024-49894	CVE-2022-49874
CVE-2024-49895	CVE-2022-49875
CVE-2024-49896	CVE-2022-49878
CVE-2024-49900	CVE-2022-49880
CVE-2024-49902	CVE-2022-49881
CVE-2024-49903	CVE-2022-49885
CVE-2024-49907	CVE-2022-49887
CVE-2024-49913	CVE-2022-49888
CVE-2024-49924	CVE-2022-49890
CVE-2024-49927	CVE-2022-49891
CVE-2024-49930	CVE-2022-49892
CVE-2024-49933	CVE-2022-49899
CVE-2024-49935	CVE-2022-49902
CVE-2024-49936	CVE-2022-49904
CVE-2024-49938	CVE-2022-49906
CVE-2024-49944	CVE-2022-49908
CVE-2024-49946	CVE-2022-49909
CVE-2024-49948	CVE-2022-49915
CVE-2024-49949	CVE-2022-49916
CVE-2024-49952	CVE-2022-49919
CVE-2024-49954	CVE-2022-49920
CVE-2024-49955	CVE-2022-49921
CVE-2024-49957	CVE-2022-49922
CVE-2024-49958	CVE-2022-49923
CVE-2024-49959	CVE-2022-49924
CVE-2024-49962	CVE-2022-49925
CVE-2024-49963	CVE-2022-49926
CVE-2024-49965	CVE-2022-49927
CVE-2024-49966	CVE-2022-49928
CVE-2024-49969	CVE-2022-49931
CVE-2024-49973	CVE-2023-0045
CVE-2024-49975	CVE-2023-0179
CVE-2024-49977	CVE-2023-0210
CVE-2024-49981	CVE-2023-0266
CVE-2024-49982	CVE-2023-0386
CVE-2024-49983	CVE-2023-0459
CVE-2024-49985	CVE-2023-0461
CVE-2024-49997	CVE-2023-1077
CVE-2024-50000	CVE-2023-1078
CVE-2024-50001	CVE-2023-1118
CVE-2024-50002	CVE-2023-1194
CVE-2024-50003	CVE-2023-1281
CVE-2024-50006	CVE-2023-1380
CVE-2024-50007	CVE-2023-1611
CVE-2024-50008	CVE-2023-1652
CVE-2024-50013	CVE-2023-1670
CVE-2024-50015	CVE-2023-1829
CVE-2024-50019	CVE-2023-1989
CVE-2024-50024	CVE-2023-2006
CVE-2024-50031	CVE-2023-2156
CVE-2024-50033	CVE-2023-2163
CVE-2024-50035	CVE-2023-2235
CVE-2024-50038	CVE-2023-23559
CVE-2024-50039	CVE-2023-26544
CVE-2024-50040	CVE-2023-26606
CVE-2024-50041	CVE-2023-26607
CVE-2024-50044	CVE-2023-28466

CVE-2024-50045	CVE-2023-3090
CVE-2024-50046	CVE-2023-31248
CVE-2024-50049	CVE-2023-3141
CVE-2024-50051	CVE-2023-31436
CVE-2024-50059	CVE-2023-32233
CVE-2024-50062	CVE-2023-32247
CVE-2024-50074	CVE-2023-32248
CVE-2024-50082	CVE-2023-32250
CVE-2024-50083	CVE-2023-32252
CVE-2024-50093	CVE-2023-32254
CVE-2024-50095	CVE-2023-32257
CVE-2024-50096	CVE-2023-32258
CVE-2024-50099	CVE-2023-3390
CVE-2024-50101	CVE-2023-35001
CVE-2024-50103	CVE-2023-35788
CVE-2024-50110	CVE-2023-35828
CVE-2024-50115	CVE-2023-35829
CVE-2024-50116	CVE-2023-3610
CVE-2024-50117	CVE-2023-3611
CVE-2024-50127	CVE-2023-3776
CVE-2024-50128	CVE-2023-3777
CVE-2024-50131	CVE-2023-3812
CVE-2024-50134	CVE-2023-38426
CVE-2024-50141	CVE-2023-38427
CVE-2024-50142	CVE-2023-38428
CVE-2024-50143	CVE-2023-38429
CVE-2024-50148	CVE-2023-38430
CVE-2024-50150	CVE-2023-38431
CVE-2024-50151	CVE-2023-38432
CVE-2024-50153	CVE-2023-39197
CVE-2024-50154	CVE-2023-4004
CVE-2024-50156	CVE-2023-4015
CVE-2024-50160	CVE-2023-40283
CVE-2024-50162	CVE-2023-4147
CVE-2024-50163	CVE-2023-4206
CVE-2024-50167	CVE-2023-4207
CVE-2024-50168	CVE-2023-4208
CVE-2024-50171	CVE-2023-42753
CVE-2024-50179	CVE-2023-44466
CVE-2024-50180	CVE-2023-45871
CVE-2024-50182	CVE-2023-4623
CVE-2024-50184	CVE-2023-46838
CVE-2024-50185	CVE-2023-4921
CVE-2024-50186	CVE-2023-5178
CVE-2024-50188	CVE-2023-5197
CVE-2024-50189	CVE-2023-52429
CVE-2024-50191	CVE-2023-52434
CVE-2024-50192	CVE-2023-52435
CVE-2024-50193	CVE-2023-52436
CVE-2024-50194	CVE-2023-52438
CVE-2024-50195	CVE-2023-52439
CVE-2024-50196	CVE-2023-52441
CVE-2024-50198	CVE-2023-52442
CVE-2024-50201	CVE-2023-52443
CVE-2024-50202	CVE-2023-52444
CVE-2024-50205	CVE-2023-52445
CVE-2024-50208	CVE-2023-52447
CVE-2024-50209	CVE-2023-52448
CVE-2024-50229	CVE-2023-52449
CVE-2024-50230	CVE-2023-52451
CVE-2024-50232	CVE-2023-52454
CVE-2024-50233	CVE-2023-52456
CVE-2024-50234	CVE-2023-52458
CVE-2024-50236	CVE-2023-52462
CVE-2024-50237	CVE-2023-52463
CVE-2024-50244	CVE-2023-52464
CVE-2024-50245	CVE-2023-52467
CVE-2024-50247	CVE-2023-52469
CVE-2024-50251	CVE-2023-52470
CVE-2024-50257	CVE-2023-52474
CVE-2024-50259	CVE-2023-52475
CVE-2024-50262	CVE-2023-52476
CVE-2024-50264	CVE-2023-52477
CVE-2024-50265	CVE-2023-52478
CVE-2024-50267	CVE-2023-52479
CVE-2024-50268	CVE-2023-52480
CVE-2024-50269	CVE-2023-52482
CVE-2024-50273	CVE-2023-52483
CVE-2024-50278	CVE-2023-52484

CVE-2024-50279	CVE-2023-52486
CVE-2024-50282	CVE-2023-52489
CVE-2024-50287	CVE-2023-52491
CVE-2024-50290	CVE-2023-52492
CVE-2024-50292	CVE-2023-52493
CVE-2024-50296	CVE-2023-52494
CVE-2024-50299	CVE-2023-52497
CVE-2024-50301	CVE-2023-52498
CVE-2024-50302	CVE-2023-52499
CVE-2024-53052	CVE-2023-52500
CVE-2024-53055	CVE-2023-52501
CVE-2024-53057	CVE-2023-52502
CVE-2024-53058	CVE-2023-52503
CVE-2024-53059	CVE-2023-52504
CVE-2024-53060	CVE-2023-52507
CVE-2024-53061	CVE-2023-52509
CVE-2024-53063	CVE-2023-52510
CVE-2024-53066	CVE-2023-52511
CVE-2024-53088	CVE-2023-52513
CVE-2024-53096	CVE-2023-52515
CVE-2024-53101	CVE-2023-52516
CVE-2024-53103	CVE-2023-52517
CVE-2024-53104	CVE-2023-52519
CVE-2024-53145	CVE-2023-52520
CVE-2024-53146	CVE-2023-52522
CVE-2024-53150	CVE-2023-52523
CVE-2024-53151	CVE-2023-52527
CVE-2024-53155	CVE-2023-52528
CVE-2024-53156	CVE-2023-52529
CVE-2024-53157	CVE-2023-52530
CVE-2024-53158	CVE-2023-52531
CVE-2024-53161	CVE-2023-52559
CVE-2024-53165	CVE-2023-52563
CVE-2024-53171	CVE-2023-52566
CVE-2024-53173	CVE-2023-52572
CVE-2024-53174	CVE-2023-52573
CVE-2024-53180	CVE-2023-52574
CVE-2024-53194	CVE-2023-52578
CVE-2024-53197	CVE-2023-52580
CVE-2024-53198	CVE-2023-52583
CVE-2024-53214	CVE-2023-52587
CVE-2024-53215	CVE-2023-52588
CVE-2024-53217	CVE-2023-52594
CVE-2024-53226	CVE-2023-52595
CVE-2024-53227	CVE-2023-52597
CVE-2024-53237	CVE-2023-52598
CVE-2024-53239	CVE-2023-52599
CVE-2024-55916	CVE-2023-52600
CVE-2024-56369	CVE-2023-52601
CVE-2024-56531	CVE-2023-52602
CVE-2024-56532	CVE-2023-52603
CVE-2024-56533	CVE-2023-52604
CVE-2024-56548	CVE-2023-52606
CVE-2024-56558	CVE-2023-52607
CVE-2024-56567	CVE-2023-52608
CVE-2024-56568	CVE-2023-52609
CVE-2024-56569	CVE-2023-52610
CVE-2024-56572	CVE-2023-52612
CVE-2024-56574	CVE-2023-52614
CVE-2024-56575	CVE-2023-52615
CVE-2024-56578	CVE-2023-52616
CVE-2024-56581	CVE-2023-52617
CVE-2024-56587	CVE-2023-52618
CVE-2024-56593	CVE-2023-52619
CVE-2024-56595	CVE-2023-52620
CVE-2024-56596	CVE-2023-52621
CVE-2024-56598	CVE-2023-52622
CVE-2024-56600	CVE-2023-52623
CVE-2024-56601	CVE-2023-52627
CVE-2024-56602	CVE-2023-52628
CVE-2024-56603	CVE-2023-52631
CVE-2024-56605	CVE-2023-52633
CVE-2024-56606	CVE-2023-52635
CVE-2024-56614	CVE-2023-52637
CVE-2024-56615	CVE-2023-52638
CVE-2024-56619	CVE-2023-52640
CVE-2024-56622	CVE-2023-52641
CVE-2024-56623	CVE-2023-52642
CVE-2024-56626	CVE-2023-52643

CVE-2024-56627	CVE-2023-52644
CVE-2024-56629	CVE-2023-52645
CVE-2024-56634	CVE-2023-52646
CVE-2024-56640	CVE-2023-52650
CVE-2024-56642	CVE-2023-52652
CVE-2024-56643	CVE-2023-52655
CVE-2024-56648	CVE-2023-52662
CVE-2024-56650	CVE-2023-52667
CVE-2024-56659	CVE-2023-52674
CVE-2024-56662	CVE-2023-52679
CVE-2024-56670	CVE-2023-52691
CVE-2024-56678	CVE-2023-52696
CVE-2024-56688	CVE-2023-52698
CVE-2024-56693	CVE-2023-52699
CVE-2024-56694	CVE-2023-52702
CVE-2024-56698	CVE-2023-52705
CVE-2024-56704	CVE-2023-52707
CVE-2024-56708	CVE-2023-52708
CVE-2024-56715	CVE-2023-52735
CVE-2024-56716	CVE-2023-52738
CVE-2024-56720	CVE-2023-52741
CVE-2024-56723	CVE-2023-52744
CVE-2024-56724	CVE-2023-52745
CVE-2024-56726	CVE-2023-52746
CVE-2024-56739	CVE-2023-52752
CVE-2024-56745	CVE-2023-52753
CVE-2024-56746	CVE-2023-52755
CVE-2024-56747	CVE-2023-52757
CVE-2024-56748	CVE-2023-52763
CVE-2024-56754	CVE-2023-52766
CVE-2024-56756	CVE-2023-52768
CVE-2024-56770	CVE-2023-52772
CVE-2024-56774	CVE-2023-52789
CVE-2024-56776	CVE-2023-52798
CVE-2024-56777	CVE-2023-52799
CVE-2024-56778	CVE-2023-52800
CVE-2024-56779	CVE-2023-52805
CVE-2024-56780	CVE-2023-52806
CVE-2024-56781	CVE-2023-52808
CVE-2024-56785	CVE-2023-52809
CVE-2024-56787	CVE-2023-52810
CVE-2024-57802	CVE-2023-52811
CVE-2024-57807	CVE-2023-52812
CVE-2024-57841	CVE-2023-52814
CVE-2024-57850	CVE-2023-52815
CVE-2024-57874	CVE-2023-52817
CVE-2024-57890	CVE-2023-52818
CVE-2024-57896	CVE-2023-52819
CVE-2024-57900	CVE-2023-52821
CVE-2024-57910	CVE-2023-52825
CVE-2024-57911	CVE-2023-52826
CVE-2024-57913	CVE-2023-52832
CVE-2024-57922	CVE-2023-52833
CVE-2024-57938	CVE-2023-52840
CVE-2024-57946	CVE-2023-52841
CVE-2024-57951	CVE-2023-52844
CVE-2024-57979	CVE-2023-52845
CVE-2024-58034	CVE-2023-52846
CVE-2024-58052	CVE-2023-52849
CVE-2024-58055	CVE-2023-52852
CVE-2024-58058	CVE-2023-52854
CVE-2024-58063	CVE-2023-52855
CVE-2024-58069	CVE-2023-52856
CVE-2024-58071	CVE-2023-52858
CVE-2024-58076	CVE-2023-52859
CVE-2024-58083	CVE-2023-52863
CVE-2024-58087	CVE-2023-52865
CVE-2025-21636	CVE-2023-52869
CVE-2025-21637	CVE-2023-52870
CVE-2025-21638	CVE-2023-52872
CVE-2025-21665	CVE-2023-52873
CVE-2025-21666	CVE-2023-52875
CVE-2025-21669	CVE-2023-52876
CVE-2025-21680	CVE-2023-52877
CVE-2025-21683	CVE-2023-52878
CVE-2025-21687	CVE-2023-52884
CVE-2025-21689	CVE-2023-52885
CVE-2025-21690	CVE-2023-52889
CVE-2025-21692	CVE-2023-52893

CVE-2025-21694	CVE-2023-52894
CVE-2025-21697	CVE-2023-52896
CVE-2025-21699	CVE-2023-52898
CVE-2025-21700	CVE-2023-52899
CVE-2025-21715	CVE-2023-52900
CVE-2025-21722	CVE-2023-52901
CVE-2025-21727	CVE-2023-52903
CVE-2025-21731	CVE-2023-52906
CVE-2025-21753	CVE-2023-52907
CVE-2025-21756	CVE-2023-52910
CVE-2025-21760	CVE-2023-52915
CVE-2025-21761	CVE-2023-52918
CVE-2025-21762	CVE-2023-52919
CVE-2025-21763	CVE-2023-52922
CVE-2025-21764	CVE-2023-52927
CVE-2025-21796	CVE-2023-52930
CVE-2025-21811	CVE-2023-52932
CVE-2025-21887	CVE-2023-52936
CVE-2025-21898	CVE-2023-52973
CVE-2025-21904	CVE-2023-52974
CVE-2025-21905	CVE-2023-52975
CVE-2025-21912	CVE-2023-52976
CVE-2025-21917	CVE-2023-52978
CVE-2025-21919	CVE-2023-52979
CVE-2025-21920	CVE-2023-52984
CVE-2025-21922	CVE-2023-52988
CVE-2025-21928	CVE-2023-52989
CVE-2025-21934	CVE-2023-52991
CVE-2025-21941	CVE-2023-52993
CVE-2025-21943	CVE-2023-53003
CVE-2025-21948	CVE-2023-53005
CVE-2025-21951	CVE-2023-53011
CVE-2025-21957	CVE-2023-53013
CVE-2025-21959	CVE-2023-53015
CVE-2025-21962	CVE-2023-53016
CVE-2025-21963	CVE-2023-53020
CVE-2025-21964	CVE-2023-53021
CVE-2025-21968	CVE-2023-53022
CVE-2025-21996	CVE-2023-53023
CVE-2025-22018	CVE-2023-53026
CVE-2025-22020	CVE-2023-5717
CVE-2025-22035	CVE-2023-6040
CVE-2025-22054	CVE-2023-6356
CVE-2025-22056	CVE-2023-6536
CVE-2025-22063	CVE-2023-6817
CVE-2025-22066	CVE-2023-6932
CVE-2025-22081	CVE-2024-0562
CVE-2025-22097	CVE-2024-0646
CVE-2025-23136	CVE-2024-0841
CVE-2025-37785	CVE-2024-1085
CVE-2025-37803	CVE-2024-1086
CVE-2025-37805	CVE-2024-26586
CVE-2025-38152	CVE-2024-26589
CVE-2025-38352	CVE-2024-26591
CVE-2025-39728	CVE-2024-26592
CVE-2024-52533	CVE-2024-26593
CVE-2025-57052	CVE-2024-26594
CVE-2022-0367	CVE-2024-26597
CVE-2024-36843	CVE-2024-26598
CVE-2024-36844	CVE-2024-26600
CVE-2024-36845	CVE-2024-26601
CVE-2024-47619	CVE-2024-26602
CVE-2024-23337	CVE-2024-26603
CVE-2024-53427	CVE-2024-26606
CVE-2025-48060	CVE-2024-26608
	CVE-2024-26610
	CVE-2024-26614
	CVE-2024-26615
	CVE-2024-26622
	CVE-2024-26625
	CVE-2024-26627
	CVE-2024-26631
	CVE-2024-26633
	CVE-2024-26635
	CVE-2024-26636
	CVE-2024-26640
	CVE-2024-26641
	CVE-2024-26642
	CVE-2024-26643

	CVE-2024-26644
	CVE-2024-26645
	CVE-2024-26651
	CVE-2024-26654
	CVE-2024-26659
	CVE-2024-26660
	CVE-2024-26663
	CVE-2024-26665
	CVE-2024-26668
	CVE-2024-26671
	CVE-2024-26673
	CVE-2024-26675
	CVE-2024-26679
	CVE-2024-26684
	CVE-2024-26685
	CVE-2024-26688
	CVE-2024-26689
	CVE-2024-26695
	CVE-2024-26696
	CVE-2024-26697
	CVE-2024-26698
	CVE-2024-26702
	CVE-2024-26704
	CVE-2024-26707
	CVE-2024-26712
	CVE-2024-26715
	CVE-2024-26717
	CVE-2024-26727
	CVE-2024-26733
	CVE-2024-26735
	CVE-2024-26736
	CVE-2024-26737
	CVE-2024-26739
	CVE-2024-26743
	CVE-2024-26744
	CVE-2024-26747
	CVE-2024-26748
	CVE-2024-26749
	CVE-2024-26751
	CVE-2024-26754
	CVE-2024-26763
	CVE-2024-26764
	CVE-2024-26769
	CVE-2024-26771
	CVE-2024-26772
	CVE-2024-26773
	CVE-2024-26774
	CVE-2024-26776
	CVE-2024-26777
	CVE-2024-26778
	CVE-2024-26779
	CVE-2024-26782
	CVE-2024-26787
	CVE-2024-26788
	CVE-2024-26790
	CVE-2024-26791
	CVE-2024-26793
	CVE-2024-26795
	CVE-2024-26798
	CVE-2024-26801
	CVE-2024-26802
	CVE-2024-26803
	CVE-2024-26804
	CVE-2024-26805
	CVE-2024-26808
	CVE-2024-26809
	CVE-2024-26810
	CVE-2024-26813
	CVE-2024-26816
	CVE-2024-26817
	CVE-2024-26825
	CVE-2024-26826
	CVE-2024-26829
	CVE-2024-26833
	CVE-2024-26835
	CVE-2024-26838
	CVE-2024-26839
	CVE-2024-26840
	CVE-2024-26843

	CVE-2024-26845
	CVE-2024-26846
	CVE-2024-26851
	CVE-2024-26852
	CVE-2024-26855
	CVE-2024-26856
	CVE-2024-26857
	CVE-2024-26859
	CVE-2024-26861
	CVE-2024-26862
	CVE-2024-26863
	CVE-2024-26870
	CVE-2024-26872
	CVE-2024-26874
	CVE-2024-26875
	CVE-2024-26878
	CVE-2024-26879
	CVE-2024-26881
	CVE-2024-26882
	CVE-2024-26883
	CVE-2024-26884
	CVE-2024-26885
	CVE-2024-26891
	CVE-2024-26894
	CVE-2024-26895
	CVE-2024-26898
	CVE-2024-26901
	CVE-2024-26903
	CVE-2024-26906
	CVE-2024-26907
	CVE-2024-26910
	CVE-2024-26914
	CVE-2024-26915
	CVE-2024-26921
	CVE-2024-26924
	CVE-2024-26928
	CVE-2024-26931
	CVE-2024-26934
	CVE-2024-26936
	CVE-2024-26944
	CVE-2024-26950
	CVE-2024-26952
	CVE-2024-26957
	CVE-2024-26958
	CVE-2024-26960
	CVE-2024-26961
	CVE-2024-26964
	CVE-2024-26966
	CVE-2024-26969
	CVE-2024-26970
	CVE-2024-26973
	CVE-2024-26974
	CVE-2024-26976
	CVE-2024-26977
	CVE-2024-26980
	CVE-2024-26981
	CVE-2024-26984
	CVE-2024-26989
	CVE-2024-26993
	CVE-2024-26996
	CVE-2024-26999
	CVE-2024-27009
	CVE-2024-27013
	CVE-2024-27014
	CVE-2024-27015
	CVE-2024-27016
	CVE-2024-27019
	CVE-2024-27020
	CVE-2024-27024
	CVE-2024-27025
	CVE-2024-27028
	CVE-2024-27030
	CVE-2024-27034
	CVE-2024-27037
	CVE-2024-27038
	CVE-2024-27039
	CVE-2024-27043
	CVE-2024-27044
	CVE-2024-27045

	CVE-2024-27046
	CVE-2024-27047
	CVE-2024-27051
	CVE-2024-27052
	CVE-2024-27053
	CVE-2024-27054
	CVE-2024-27059
	CVE-2024-27072
	CVE-2024-27073
	CVE-2024-27074
	CVE-2024-27076
	CVE-2024-27077
	CVE-2024-27078
	CVE-2024-27388
	CVE-2024-27390
	CVE-2024-27393
	CVE-2024-27395
	CVE-2024-27396
	CVE-2024-27397
	CVE-2024-27402
	CVE-2024-27403
	CVE-2024-27405
	CVE-2024-34027
	CVE-2024-34777
	CVE-2024-35247
	CVE-2024-35804
	CVE-2024-35806
	CVE-2024-35811
	CVE-2024-35823
	CVE-2024-35828
	CVE-2024-35829
	CVE-2024-35833
	CVE-2024-35835
	CVE-2024-35845
	CVE-2024-35847
	CVE-2024-35849
	CVE-2024-35851
	CVE-2024-35852
	CVE-2024-35853
	CVE-2024-35854
	CVE-2024-35855
	CVE-2024-35857
	CVE-2024-35866
	CVE-2024-35867
	CVE-2024-35869
	CVE-2024-35885
	CVE-2024-35888
	CVE-2024-35895
	CVE-2024-35896
	CVE-2024-35898
	CVE-2024-35899
	CVE-2024-35907
	CVE-2024-35915
	CVE-2024-35922
	CVE-2024-35925
	CVE-2024-35930
	CVE-2024-35933
	CVE-2024-35940
	CVE-2024-35947
	CVE-2024-35955
	CVE-2024-35960
	CVE-2024-35969
	CVE-2024-35970
	CVE-2024-35972
	CVE-2024-35973
	CVE-2024-35976
	CVE-2024-35978
	CVE-2024-35982
	CVE-2024-35984
	CVE-2024-35989
	CVE-2024-35990
	CVE-2024-35997
	CVE-2024-36008
	CVE-2024-36014
	CVE-2024-36015
	CVE-2024-36016
	CVE-2024-36025
	CVE-2024-36032
	CVE-2024-36270

	CVE-2024-36286
	CVE-2024-36476
	CVE-2024-36489
	CVE-2024-36894
	CVE-2024-36897
	CVE-2024-36906
	CVE-2024-36912
	CVE-2024-36913
	CVE-2024-36923
	CVE-2024-36931
	CVE-2024-36937
	CVE-2024-36938
	CVE-2024-36940
	CVE-2024-36941
	CVE-2024-36947
	CVE-2024-36954
	CVE-2024-36955
	CVE-2024-36960
	CVE-2024-36965
	CVE-2024-36967
	CVE-2024-36969
	CVE-2024-36971
	CVE-2024-36978
	CVE-2024-37078
	CVE-2024-37356
	CVE-2024-38541
	CVE-2024-38545
	CVE-2024-38546
	CVE-2024-38547
	CVE-2024-38548
	CVE-2024-38549
	CVE-2024-38550
	CVE-2024-38552
	CVE-2024-38555
	CVE-2024-38559
	CVE-2024-38560
	CVE-2024-38571
	CVE-2024-38573
	CVE-2024-38577
	CVE-2024-38578
	CVE-2024-38582
	CVE-2024-38583
	CVE-2024-38586
	CVE-2024-38588
	CVE-2024-38589
	CVE-2024-38590
	CVE-2024-38591
	CVE-2024-38596
	CVE-2024-38597
	CVE-2024-38599
	CVE-2024-38600
	CVE-2024-38601
	CVE-2024-38605
	CVE-2024-38610
	CVE-2024-38612
	CVE-2024-38613
	CVE-2024-38621
	CVE-2024-38623
	CVE-2024-38627
	CVE-2024-38633
	CVE-2024-38635
	CVE-2024-38637
	CVE-2024-38661
	CVE-2024-38662
	CVE-2024-38780
	CVE-2024-39276
	CVE-2024-39277
	CVE-2024-39292
	CVE-2024-39301
	CVE-2024-39463
	CVE-2024-39466
	CVE-2024-39467
	CVE-2024-39468
	CVE-2024-39471
	CVE-2024-39475
	CVE-2024-39476
	CVE-2024-39480
	CVE-2024-39482
	CVE-2024-39484

	CVE-2024-39487
	CVE-2024-39488
	CVE-2024-39489
	CVE-2024-39490
	CVE-2024-39494
	CVE-2024-39495
	CVE-2024-39497
	CVE-2024-39499
	CVE-2024-39500
	CVE-2024-39502
	CVE-2024-39505
	CVE-2024-39506
	CVE-2024-39507
	CVE-2024-39509
	CVE-2024-40901
	CVE-2024-40902
	CVE-2024-40904
	CVE-2024-40905
	CVE-2024-40911
	CVE-2024-40912
	CVE-2024-40927
	CVE-2024-40929
	CVE-2024-40931
	CVE-2024-40932
	CVE-2024-40942
	CVE-2024-40943
	CVE-2024-40945
	CVE-2024-40953
	CVE-2024-40954
	CVE-2024-40956
	CVE-2024-40957
	CVE-2024-40958
	CVE-2024-40959
	CVE-2024-40960
	CVE-2024-40961
	CVE-2024-40967
	CVE-2024-40968
	CVE-2024-40970
	CVE-2024-40974
	CVE-2024-40978
	CVE-2024-40980
	CVE-2024-40981
	CVE-2024-40984
	CVE-2024-40994
	CVE-2024-40995
	CVE-2024-41000
	CVE-2024-41002
	CVE-2024-41007
	CVE-2024-41011
	CVE-2024-41012
	CVE-2024-41040
	CVE-2024-41046
	CVE-2024-41048
	CVE-2024-41059
	CVE-2024-41060
	CVE-2024-41061
	CVE-2024-41063
	CVE-2024-41064
	CVE-2024-41070
	CVE-2024-41073
	CVE-2024-41077
	CVE-2024-41087
	CVE-2024-41089
	CVE-2024-41092
	CVE-2024-41093
	CVE-2024-41095
	CVE-2024-41097
	CVE-2024-42068
	CVE-2024-42070
	CVE-2024-42076
	CVE-2024-42077
	CVE-2024-42080
	CVE-2024-42082
	CVE-2024-42089
	CVE-2024-42090
	CVE-2024-42093
	CVE-2024-42094
	CVE-2024-42101
	CVE-2024-42104

	CVE-2024-42106
	CVE-2024-42114
	CVE-2024-42131
	CVE-2024-42145
	CVE-2024-42148
	CVE-2024-42152
	CVE-2024-42153
	CVE-2024-42154
	CVE-2024-42157
	CVE-2024-42161
	CVE-2024-42223
	CVE-2024-42224
	CVE-2024-42225
	CVE-2024-42229
	CVE-2024-42232
	CVE-2024-42236
	CVE-2024-42244
	CVE-2024-42247
	CVE-2024-42259
	CVE-2024-42271
	CVE-2024-42280
	CVE-2024-42283
	CVE-2024-42284
	CVE-2024-42285
	CVE-2024-42286
	CVE-2024-42288
	CVE-2024-42289
	CVE-2024-42292
	CVE-2024-42301
	CVE-2024-42302
	CVE-2024-42309
	CVE-2024-42310
	CVE-2024-42311
	CVE-2024-42313
	CVE-2024-43098
	CVE-2024-43817
	CVE-2024-43828
	CVE-2024-43854
	CVE-2024-43856
	CVE-2024-43858
	CVE-2024-43860
	CVE-2024-43861
	CVE-2024-43863
	CVE-2024-43871
	CVE-2024-43873
	CVE-2024-43882
	CVE-2024-43889
	CVE-2024-43890
	CVE-2024-43893
	CVE-2024-43894
	CVE-2024-43895
	CVE-2024-43902
	CVE-2024-43907
	CVE-2024-43908
	CVE-2024-43909
	CVE-2024-43914
	CVE-2024-44934
	CVE-2024-44935
	CVE-2024-44944
	CVE-2024-44947
	CVE-2024-44954
	CVE-2024-44958
	CVE-2024-44960
	CVE-2024-44965
	CVE-2024-44966
	CVE-2024-44969
	CVE-2024-44971
	CVE-2024-44972
	CVE-2024-44982
	CVE-2024-44983
	CVE-2024-44985
	CVE-2024-44986
	CVE-2024-44987
	CVE-2024-44988
	CVE-2024-44989
	CVE-2024-44990
	CVE-2024-44995
	CVE-2024-44998
	CVE-2024-44999

	CVE-2024-45003
	CVE-2024-45006
	CVE-2024-45009
	CVE-2024-45011
	CVE-2024-45016
	CVE-2024-45018
	CVE-2024-45021
	CVE-2024-45025
	CVE-2024-45026
	CVE-2024-45028
	CVE-2024-45828
	CVE-2024-46673
	CVE-2024-46674
	CVE-2024-46675
	CVE-2024-46676
	CVE-2024-46677
	CVE-2024-46679
	CVE-2024-46685
	CVE-2024-46689
	CVE-2024-46702
	CVE-2024-46707
	CVE-2024-46714
	CVE-2024-46719
	CVE-2024-46721
	CVE-2024-46722
	CVE-2024-46723
	CVE-2024-46724
	CVE-2024-46725
	CVE-2024-46731
	CVE-2024-46732
	CVE-2024-46737
	CVE-2024-46738
	CVE-2024-46739
	CVE-2024-46740
	CVE-2024-46743
	CVE-2024-46744
	CVE-2024-46746
	CVE-2024-46747
	CVE-2024-46750
	CVE-2024-46755
	CVE-2024-46759
	CVE-2024-46761
	CVE-2024-46763
	CVE-2024-46771
	CVE-2024-46777
	CVE-2024-46780
	CVE-2024-46781
	CVE-2024-46782
	CVE-2024-46783
	CVE-2024-46791
	CVE-2024-46795
	CVE-2024-46798
	CVE-2024-46800
	CVE-2024-46804
	CVE-2024-46805
	CVE-2024-46807
	CVE-2024-46810
	CVE-2024-46814
	CVE-2024-46815
	CVE-2024-46817
	CVE-2024-46818
	CVE-2024-46819
	CVE-2024-46822
	CVE-2024-46828
	CVE-2024-46829
	CVE-2024-46832
	CVE-2024-46840
	CVE-2024-46844
	CVE-2024-47143
	CVE-2024-47659
	CVE-2024-47660
	CVE-2024-47663
	CVE-2024-47665
	CVE-2024-47667
	CVE-2024-47668
	CVE-2024-47669
	CVE-2024-47672
	CVE-2024-47674
	CVE-2024-47679

	CVE-2024-47684
	CVE-2024-47685
	CVE-2024-47690
	CVE-2024-47692
	CVE-2024-47693
	CVE-2024-47695
	CVE-2024-47697
	CVE-2024-47698
	CVE-2024-47699
	CVE-2024-47701
	CVE-2024-47705
	CVE-2024-47706
	CVE-2024-47710
	CVE-2024-47713
	CVE-2024-47718
	CVE-2024-47720
	CVE-2024-47723
	CVE-2024-47734
	CVE-2024-47735
	CVE-2024-47737
	CVE-2024-47739
	CVE-2024-47742
	CVE-2024-47747
	CVE-2024-47748
	CVE-2024-47749
	CVE-2024-47757
	CVE-2024-49851
	CVE-2024-49852
	CVE-2024-49854
	CVE-2024-49856
	CVE-2024-49858
	CVE-2024-49860
	CVE-2024-49863
	CVE-2024-49866
	CVE-2024-49867
	CVE-2024-49868
	CVE-2024-49871
	CVE-2024-49875
	CVE-2024-49877
	CVE-2024-49878
	CVE-2024-49879
	CVE-2024-49881
	CVE-2024-49882
	CVE-2024-49883
	CVE-2024-49884
	CVE-2024-49889
	CVE-2024-49890
	CVE-2024-49892
	CVE-2024-49894
	CVE-2024-49895
	CVE-2024-49896
	CVE-2024-49900
	CVE-2024-49902
	CVE-2024-49903
	CVE-2024-49907
	CVE-2024-49913
	CVE-2024-49924
	CVE-2024-49927
	CVE-2024-49930
	CVE-2024-49933
	CVE-2024-49935
	CVE-2024-49936
	CVE-2024-49938
	CVE-2024-49944
	CVE-2024-49946
	CVE-2024-49948
	CVE-2024-49949
	CVE-2024-49952
	CVE-2024-49954
	CVE-2024-49955
	CVE-2024-49957
	CVE-2024-49958
	CVE-2024-49959
	CVE-2024-49962
	CVE-2024-49963
	CVE-2024-49965
	CVE-2024-49966
	CVE-2024-49969
	CVE-2024-49973

	CVE-2024-49975
	CVE-2024-49981
	CVE-2024-49983
	CVE-2024-49985
	CVE-2024-49997
	CVE-2024-50000
	CVE-2024-50001
	CVE-2024-50002
	CVE-2024-50003
	CVE-2024-50006
	CVE-2024-50007
	CVE-2024-50008
	CVE-2024-50013
	CVE-2024-50015
	CVE-2024-50019
	CVE-2024-50024
	CVE-2024-50031
	CVE-2024-50033
	CVE-2024-50035
	CVE-2024-50038
	CVE-2024-50039
	CVE-2024-50041
	CVE-2024-50044
	CVE-2024-50045
	CVE-2024-50046
	CVE-2024-50049
	CVE-2024-50051
	CVE-2024-50059
	CVE-2024-50062
	CVE-2024-50074
	CVE-2024-50082
	CVE-2024-50083
	CVE-2024-50093
	CVE-2024-50095
	CVE-2024-50096
	CVE-2024-50099
	CVE-2024-50103
	CVE-2024-50110
	CVE-2024-50115
	CVE-2024-50116
	CVE-2024-50117
	CVE-2024-50127
	CVE-2024-50128
	CVE-2024-50131
	CVE-2024-50134
	CVE-2024-50141
	CVE-2024-50142
	CVE-2024-50143
	CVE-2024-50148
	CVE-2024-50150
	CVE-2024-50151
	CVE-2024-50153
	CVE-2024-50154
	CVE-2024-50156
	CVE-2024-50160
	CVE-2024-50162
	CVE-2024-50163
	CVE-2024-50167
	CVE-2024-50168
	CVE-2024-50171
	CVE-2024-50179
	CVE-2024-50180
	CVE-2024-50182
	CVE-2024-50184
	CVE-2024-50185
	CVE-2024-50188
	CVE-2024-50189
	CVE-2024-50191
	CVE-2024-50192
	CVE-2024-50193
	CVE-2024-50194
	CVE-2024-50195
	CVE-2024-50196
	CVE-2024-50198
	CVE-2024-50201
	CVE-2024-50202
	CVE-2024-50205
	CVE-2024-50208
	CVE-2024-50209

	CVE-2024-50229
	CVE-2024-50230
	CVE-2024-50232
	CVE-2024-50233
	CVE-2024-50234
	CVE-2024-50236
	CVE-2024-50237
	CVE-2024-50244
	CVE-2024-50245
	CVE-2024-50247
	CVE-2024-50251
	CVE-2024-50257
	CVE-2024-50259
	CVE-2024-50262
	CVE-2024-50264
	CVE-2024-50265
	CVE-2024-50267
	CVE-2024-50268
	CVE-2024-50269
	CVE-2024-50273
	CVE-2024-50278
	CVE-2024-50279
	CVE-2024-50282
	CVE-2024-50287
	CVE-2024-50290
	CVE-2024-50292
	CVE-2024-50296
	CVE-2024-50299
	CVE-2024-50301
	CVE-2024-50302
	CVE-2024-53052
	CVE-2024-53055
	CVE-2024-53057
	CVE-2024-53058
	CVE-2024-53059
	CVE-2024-53060
	CVE-2024-53061
	CVE-2024-53063
	CVE-2024-53066
	CVE-2024-53088
	CVE-2024-53101
	CVE-2024-53103
	CVE-2024-53104
	CVE-2024-53145
	CVE-2024-53146
	CVE-2024-53150
	CVE-2024-53151
	CVE-2024-53155
	CVE-2024-53156
	CVE-2024-53157
	CVE-2024-53158
	CVE-2024-53161
	CVE-2024-53165
	CVE-2024-53171
	CVE-2024-53173
	CVE-2024-53174
	CVE-2024-53180
	CVE-2024-53194
	CVE-2024-53197
	CVE-2024-53198
	CVE-2024-53214
	CVE-2024-53215
	CVE-2024-53217
	CVE-2024-53227
	CVE-2024-53239
	CVE-2024-55916
	CVE-2024-56369
	CVE-2024-56531
	CVE-2024-56532
	CVE-2024-56533
	CVE-2024-56548
	CVE-2024-56558
	CVE-2024-56567
	CVE-2024-56568
	CVE-2024-56569
	CVE-2024-56572
	CVE-2024-56574
	CVE-2024-56575
	CVE-2024-56578

	CVE-2024-56581
	CVE-2024-56587
	CVE-2024-56593
	CVE-2024-56595
	CVE-2024-56596
	CVE-2024-56598
	CVE-2024-56600
	CVE-2024-56601
	CVE-2024-56602
	CVE-2024-56603
	CVE-2024-56605
	CVE-2024-56606
	CVE-2024-56614
	CVE-2024-56615
	CVE-2024-56619
	CVE-2024-56622
	CVE-2024-56623
	CVE-2024-56626
	CVE-2024-56627
	CVE-2024-56629
	CVE-2024-56634
	CVE-2024-56640
	CVE-2024-56642
	CVE-2024-56643
	CVE-2024-56648
	CVE-2024-56650
	CVE-2024-56659
	CVE-2024-56662
	CVE-2024-56670
	CVE-2024-56678
	CVE-2024-56688
	CVE-2024-56693
	CVE-2024-56698
	CVE-2024-56704
	CVE-2024-56708
	CVE-2024-56715
	CVE-2024-56716
	CVE-2024-56720
	CVE-2024-56723
	CVE-2024-56724
	CVE-2024-56726
	CVE-2024-56728
	CVE-2024-56739
	CVE-2024-56745
	CVE-2024-56746
	CVE-2024-56747
	CVE-2024-56748
	CVE-2024-56754
	CVE-2024-56756
	CVE-2024-56770
	CVE-2024-56774
	CVE-2024-56776
	CVE-2024-56777
	CVE-2024-56778
	CVE-2024-56779
	CVE-2024-56781
	CVE-2024-56785
	CVE-2024-56787
	CVE-2024-57802
	CVE-2024-57807
	CVE-2024-57850
	CVE-2024-57874
	CVE-2024-57890
	CVE-2024-57896
	CVE-2024-57900
	CVE-2024-57910
	CVE-2024-57911
	CVE-2024-57913
	CVE-2024-57922
	CVE-2024-57938
	CVE-2024-57946
	CVE-2024-57979
	CVE-2024-58034
	CVE-2024-58052
	CVE-2024-58055
	CVE-2024-58058
	CVE-2024-58063
	CVE-2024-58069
	CVE-2024-58071

	CVE-2024-58076
	CVE-2024-58083
	CVE-2024-58087
	CVE-2025-21636
	CVE-2025-21637
	CVE-2025-21638
	CVE-2025-21665
	CVE-2025-21666
	CVE-2025-21669
	CVE-2025-21680
	CVE-2025-21683
	CVE-2025-21687
	CVE-2025-21689
	CVE-2025-21690
	CVE-2025-21692
	CVE-2025-21697
	CVE-2025-21699
	CVE-2025-21700
	CVE-2025-21715
	CVE-2025-21722
	CVE-2025-21726
	CVE-2025-21727
	CVE-2025-21731
	CVE-2025-21753
	CVE-2025-21756
	CVE-2025-21760
	CVE-2025-21761
	CVE-2025-21762
	CVE-2025-21763
	CVE-2025-21764
	CVE-2025-21796
	CVE-2025-21811
	CVE-2025-21898
	CVE-2025-21904
	CVE-2025-21905
	CVE-2025-21912
	CVE-2025-21917
	CVE-2025-21919
	CVE-2025-21920
	CVE-2025-21922
	CVE-2025-21928
	CVE-2025-21934
	CVE-2025-21941
	CVE-2025-21943
	CVE-2025-21948
	CVE-2025-21951
	CVE-2025-21957
	CVE-2025-21959
	CVE-2025-21963
	CVE-2025-21964
	CVE-2025-21968
	CVE-2025-21996
	CVE-2025-22018
	CVE-2025-22020
	CVE-2025-22056
	CVE-2025-22063
	CVE-2025-22066
	CVE-2025-22081
	CVE-2025-22097
	CVE-2025-23136
	CVE-2025-37785
	CVE-2025-37803
	CVE-2025-37805
	CVE-2025-38152
	CVE-2025-39728
	CVE-2022-0367
	CVE-2024-36843
	CVE-2024-36844
	CVE-2024-36845
	CVE-2006-3082
	CVE-2011-2207
	CVE-2014-3591
	CVE-2014-4617
	CVE-2015-0837
	CVE-2015-1606
	CVE-2015-1607
	CVE-2016-6313
	CVE-2018-12020
	CVE-2019-13050

	CVE-2019-14855
	CVE-2022-3219
	CVE-2022-34903
	CVE-2024-10525
	CVE-2024-3935
	CVE-2024-8376
	CVE-2014-6271
	CVE-2014-7169
	CVE-2016-7543
	CVE-2016-9401
	CVE-2019-18276
	CVE-2019-9924
	CVE-2024-11053
	CVE-2024-9681
	CVE-2025-0167
	CVE-2024-47619