Q2 2026 Release Notes

This release incorporates the latest DISA STIG updates from the April 2026 quarterly release cycle and adds the newly released STIG benchmarks: **Microsoft Windows Server 2025** and **Red Hat Enterprise Linux 10**.

112	22	2	15
STIGID UPDATES	BENCHMARK UPDATES	NEW BENCHMARKS	SEVERITY CHANGES

New Benchmarks

Microsoft Windows Server 2025 - V1R1

Initial Release

DISA published the initial Windows Server 2025 STIG on 26 January 2026.

Red Hat Enterprise Linux 10 - V1R1

Initial Release

DISA published the initial RHEL 10 STIG on 26 February 2026.

DISA STIG Updates (April 2026)

The following summarizes key changes from DISA's quarterly STIG release dated 01 April 2026.

RHEL 8 - V2R7

↑ Severity Upgrades (CAT II → CAT I)

DISA elevated SSH FIPS, BIND FIPS, and IPsec FIPS requirements to CAT I: `RHEL-08-010275`, `RHEL-08-010280`, `RHEL-08-010290`, `RHEL-08-010291`, `RHEL-08-010296`, `RHEL-08-010297`.

Key Changes

- `RHEL-08-040010` - Severity downgraded from CAT I to CAT II.
- `RHEL-08-010372 / 010373 / 010375 / 010376 / 040283` - Title and wording refresh on kernel hardening sysctls.
- `RHEL-08-010572 / 010580` - Removed vfat exception note.
- `RHEL-08-020010 / 020012 / 020016 / 020018 / 020020 / 020022` - Removed centralized account management exception note from account lockout family.
- `RHEL-08-040285` - Corrected reverse path filtering check to reference `net.ipv4.conf.all.rp_filter`.

RHEL 9 - V2R8

↑ Severity Upgrades (CAT II → CAT I)

SSH MACs/Ciphers, IPsec FIPS, BIND, and crypto-policies STIGs elevated to CAT I: **RHEL-09-215100**, **RHEL-09-215105**, **RHEL-09-255064**, **RHEL-09-255065**, **RHEL-09-255070**, **RHEL-09-255075**, **RHEL-09-671020**, **RHEL-09-672050**.

Key Changes

- **RHEL-09-212010** - Added "Not applicable to UEFI systems" note.
- **RHEL-09-215010** - Added "Not applicable if not internet connected" note.
- **RHEL-09-231105 / 231200** - Removed vfat exception note.
- **RHEL-09-252025** - Added "Not applicable if serving as NTP server" note.
- **RHEL-09-411025 / 411065 / 411070 / 232045 / 232050 / 412055 / 412060 / 412070** - Example user name updated.
- **RHEL-09-671010** - Updated FIPS verification command.

Canonical Ubuntu 22.04 LTS - V2R8

Key Changes

- **UBTU-22-232080 / 232085 / 232090 / 232095** - Updated systemd journal directory and file permission requirements.
- **UBTU-22-251020** - Updated UFW service verification command.
- **UBTU-22-271030** - Updated Ctrl-Alt-Delete disable procedure.

Canonical Ubuntu 24.04 LTS - V1R5

Key Changes

- **UBTU-24-300025** - Updated Ctrl-Alt-Delete disable procedure.
- **UBTU-24-700020 / 700060 / 700070 / 700080 / 700090** - Updated systemd journal permission requirements.

Cisco IOS Router/Switch & IOS-XE Router/Switch NDM - V3R6 / V3R7

Key Changes

- **CISC-ND-000090 / 000100 / 000120 / 000330 / 000880 / 001250 / 001270** - Added `logging size`, syslog notification, and `hidekeys` to standard archive log config.
- **CISC-ND-000010** - Added `session-limit` as alternative to `max-connections`.
- **CISC-RT-000010** - Added VRF segmentation NA note.

Cisco IOS-XR Router NDM - V3R6

Key Changes

- **CISC-ND-000980** - Added off-box syslog forwarding requirement.
- **CISC-ND-001370** - Updated Fix text to use named auth lists with `aaa group server radius`.
- **CISC-ND-001410** - Clarified EEM applet automatic backup requirements.

Microsoft Defender Antivirus - V2R8

Key Changes

- Streamlined Fix text for 25 ASR, Configuration, Cloud Protection, and Scanning STIGs (**WNDF-AV-000043** through **WNDF-AV-000077**).

- `WNDF-AV-000068` - Added "Not applicable to desktops" note.

Microsoft Windows 11 - V2R7 / Server 2019 - V3R8 / Server 2022 - V2R8

Key Changes

- `WN11-00-000031`, `WN11-00-000045`, `WN11-00-000210` - Registry path formatting and wording cleanup.
- `WN11-AU-000505`, `WN19-CC-000280`, `WN22-CC-000280` - Expanded "NA" to "not applicable" with explanatory context.
- `WN19-00-000120`, `WN22-00-000120` - Updated Host Intrusion Detection rule wording.
- `WN19-00-000270`, `WN22-00-000270` - Refined `Get-WindowsFeature` command to filter installed features.

MS SQL Server 2016 V3R5 / SQL Server 2022 Database V1R3 / Instance V1R4

Key Changes

- `SQL6-D0-003300`, `SQLD-22-003300` - Expanded TDE verification SQL query.
- `SQLI-22-009500` - Added "(AO)" abbreviation.

Microsoft Windows Server DNS - V2R4

Key Changes

- `WDNS-22-000039` - Narrowed verification path to `%ALLUSERSPROFILE%\Microsoft\Crypto\Keys`.

</> StigSanctum Script Updates

The following scripts were updated to align with revised DISA CheckContent procedures:

Windows DNS Private Key Permissions Check

Affected STIGs: `WDNS-22-000039`

Change: Updated to scan the narrowed DNSSEC private key folder per revised DISA guidance. Recursive permission check covers subfolders and files. Findings raised when any non-administrative principal has greater than read access.

Cisco Redundant Authentication Servers Check

Affected STIGs: `CISC-ND-001370`

Change: Updated to recognize named authentication lists (in addition to the prior default-list check) per revised DISA guidance. Matches DISA's updated example syntax for redundant AAA server configuration.

RHEL FIPS Mode Verification

Affected STIGs: `RHEL-09-671010`

Change: Updated to use DISA's revised single-line FIPS verification command for faster, more reliable validation across RHEL 9 systems.

Additional DISA Changes Reviewed

The following DISA changes were reviewed and confirmed that existing StigSanctum scan logic already handles the updated requirements correctly. No scan updates were needed:

- `SQL6-D0-003300`, `SQLD-22-003300` - TDE verification query expanded (existing scan already performs equivalent join, system database filter, and key algorithm check)
- `CISC-ND-000010` - Session-limit added as alternative to vty restrictions (scan already accepts both)
- `CISC-ND-001410` - EEM applet wording clarified (existing pattern still matches)
- `SQLI-22-009500` - "(AO)" abbreviation added to wording (scan logic unchanged)

Repository Improvements

Recent development activity and platform enhancements since Q1:

Web Dashboard

- New browser dashboard providing a modern interface, with the existing WPF GUIs retained as a fallback option
- Pages: Dashboard, Assets, Benchmarks, Findings, STIG Browser, Scan, Remediation, Export, History, Docs, Security, Admin
- Audit Log for security event tracking
- Fully offline; no external dependencies or webserver requirements

Remediation Engine Expansion

- 14 engine types covering more than 4,000 STIGs (over 80% automated coverage)
- Scanning engine with parallel execution for Cisco and Juniper devices
- Linux Ansible integration for RHEL and Ubuntu remediation

Trial Product Build

- Curated benchmark coverage of seven STIG Benchmarks for trial review

↑ Upgrade Instructions

Upgrade Steps

1. Back up your StigSanctum database
2. Run the installer and select the Upgrade option
3. Update the StigSanctum PowerShell module on any remote scan servers
4. Verify scan results on test systems before production rollout

Severity Reclassifications

14 RHEL FIPS and crypto-policy STIGs were upgraded from CAT II to CAT I, and 1 was downgraded from CAT I to CAT II. Findings against these StigIDs from prior scans retain their historical severity in scan history; the new severity applies to scans run after this upgrade.

Support

For questions or issues related to this release:

- Email: **support@stigsanctum.com**
- Release Notes: **www.stigsanctum.com/release-notes.html**