TANDBERG DATA

RDX QuikStation Security Patch 2026-10

Information and Instructions (QuikStation 4 / QuikStation 8)

The root fix for these vulnerabilities can only be applied to the latest firmware, 3.3.0.5, so this patch includes the update to firmware 3.3.0.5. (The patch itself can be run on every firmware version.)

1. Preface

This bulletin announces a security patch for the web management interface (Apache / PHP) of the RDX QuikStation 4 and QuikStation 8/QuikStation8_10G.

Emergency item: PHP "php2shell" vulnerabilities (CVE-2026-109618, CVE-2026-109619 / CVSS 9.2)
Critical PHP vulnerabilities disclosed on 21 October 2026. A single crafted, unauthenticated HTTP request to any URL of the web management interface (including the login page) can lead to remote code execution with the web server's privileges. The QuikStation web interface runs on Apache mod_php and is therefore affected.
This patch brings the firmware up to date and then replaces PHP with a build that contains the PHP security team's official fix (the PHP 7.4 backport), which removes the vulnerabilities themselves. Even if your unit already runs firmware 3.3.0.5, the vulnerabilities remain until this patch is applied - please apply it without fail. On some older firmware only the mitigation can be applied; **all attack techniques published or observed in the wild as of 22 October 2026 rely on the code paths that the mitigation disables, and do not succeed even against a unit with the mitigation only.** The PHP project describes the mitigation as temporary and partial, so we strongly recommend following this bulletin to bring the firmware up to date and then applying this patch again.

The patch has two layers: **(1) a mitigation** (Apache / PHP / TLS configuration changes, applicable to every firmware) and **(2) a PHP fix** (a PHP module built from PHP 7.4.33 with the PHP security team's official fix; firmware 3.3.0.5 only). A single patch is run; it applies the layers appropriate to the unit's firmware automatically. The patch also performs the update to firmware 3.3.0.5, and on units already on 3.3.0.5 the update of the spare boot slot; the unit reboots in these cases. It is applied over SSH; the web management interface restarts for a few seconds. **Except during the reboot of a firmware update, backup operation, iSCSI connections and the network link are not affected.** Do not use the unit's web console while the patch runs.

Applies to: every QuikStation 4 / QuikStation 8 / QuikStation8_10G in the field. There is no serial-number condition. What the patch does depends on the firmware:

Unit firmware	What the patch does
1.x (1.3.6–1.5.1.26)	Mitigation applied, then **one reboot to confirm the changes are stored** (see note below). To receive the PHP fix, the firmware must be updated to 2.5.2 or later (procedure linked in section 4) and the patch must be run again
2.5.2–3.2.x	Mitigation applied, then **the included firmware 3.3.0.5 is installed** (the unit reboots; a few minutes, up to about 10 on some models). After it is back, 3.3.0.5 is written into the other boot area as well, so **the unit normally reboots twice**. The Windows / macOS / Linux tools wait for each reboot and continue by themselves up to the PHP fix (only when the patch is run directly on the unit must it be run again after each reboot)
3.3.0.5	PHP fix and mitigation (if not yet applied) applied. If the other boot area holds a firmware older than 3.3.0.5, 3.3.0.5 is written there as well (**the unit reboots once**) and the PHP fix is then installed in both boot areas. If both boot areas already run 3.3.0.5, the unit **reboots once after applying to confirm the changes are stored** (see note below)

Note: some units suffer from internal storage that stops retaining writes; on such a unit every change is lost at the next reboot. Where a firmware update is performed, the reboot after it already proves that the storage keeps data. On 1.x units and on units whose both boot areas already run 3.3.0.5 nothing else reboots, so the patch reboots the unit once after applying; the re-run then shows `PERSIST: VERIFIED`. If the changes did not survive, the patch reports `STORAGE FAULT` - please contact support.

2. Items addressed by this patch

This table describes the state after this patch (firmware 3.3.0.5 + the PHP fix). Legend: **Resolved** = finding removed / Mitigated = exploitation conditions removed or impact limited. Where the result differs for a unit on firmware 1.5.1.26 or earlier that can only receive the mitigation, this is noted with (*).

Item / CVE	What the patch does	Status
CVE-2026-109618 PHP memory corruption during out-of-memory handling (RCE)	PHP replaced by PHP 7.4.33 containing the PHP security team's official fix (if a unit on firmware 1.5.1.26 or earlier can only receive the mitigation: only PHP `memory_limit = -1` and Apache `LimitRequestBody` as mitigation)	**Resolved** * mitigation only: Mitigated
CVE-2026-109619 PHP use-after-free via state retained between requests (RCE)	As above; the fixed PHP removes the session upload-progress feature altogether (if a unit on firmware 1.5.1.26 or earlier can only receive the mitigation: only PHP `session.upload_progress.enabled = 0` as mitigation)	**Resolved** * mitigation only: Mitigated

Obsolete version of PHP (PHP 7.4.5)	PHP updated to 7.4.33, the last release of the 7.4 series (including the official fix above and every fix up to 7.4.33). PHP 7.4 itself is end-of-life, so some scanners will keep flagging it as outdated (if a unit on firmware 1.5.1.26 or earlier can only receive the mitigation: stays at 7.4.5)	Updated to 7.4.33 * mitigation only: not addressed
PHP: CVE-2019-11048, CVE-2020-7068, CVE-2020-7069, CVE-2020-7070, CVE-2020-7071, CVE-2021-21702, CVE-2021-21703, CVE-2021-21704, CVE-2021-21705, CVE-2021-21707, CVE-2021-21708, CVE-2022-31625, CVE-2022-31626, CVE-2022-31628, CVE-2022-31629, CVE-2022-31630, CVE-2022-37454	Fixed in PHP 7.4.33 (if a unit on firmware 1.5.1.26 or earlier can only receive the mitigation: not addressed. Of these, CVE-2021-21702 (SOAP), 21703 (FPM), 21704 (Firebird), 2022-31625 (pgsql), 31626 (mysqlnd) and 31630 (GD) do not apply because those extensions are not loaded, CVE-2019-11048 is limited to denial of service, and the rest concern functions the web console does not use or have minor impact)	**Resolved** * mitigation only: not addressed
CVE-2024-40725 / CVE-2024-39884 Apache: source disclosure with handlers configured via AddType	PHP handler changed from `AddType` to `SetHandler` (FilesMatch)	**Resolved**
CVE-2026-79768 Apache mod_userdir information disclosure	Unused mod_userdir disabled	**Resolved**
CVE-2026-33007 Apache mod_authn_socache crash	Unused mod_authn_socache disabled	**Resolved**
CVE-2021-3449 OpenSSL NULL dereference on TLS renegotiation (DoS)	TLS ≤1.2 renegotiation disabled (`NoRenegotiation`). Firmware 1.x (OpenSSL 1.0.2) is not affected by this CVE	Mitigated
CVE-2012-4929 CRIME (TLS compression)	`SSLCompression off` made explicit	**Resolved**
TLS 1.0 / TLS 1.1 supported (RFC 8996)	Only TLS 1.2 and 1.3 allowed	**Resolved**
BEAST (CVE-2011-3389), Lucky13 (CVE-2013-0169), SWEET32 (CVE-2016-2183), Logjam / commonly used primes (CVE-2015-4000), static-key (RSA) cipher suites, weak MAC (SHA-1) cipher suites, DES/IDEA cipher suites, "no strong cipher"	Cipher suites restricted to ECDHE + AEAD (AES-GCM / ChaCha20), server order enforced, session tickets disabled	**Resolved**
Slow-request attacks (Slowloris, CVE-2007-6750)	`RequestReadTimeout` configured	Mitigated
Cross-Site Tracing (TRACE method)	`TraceEnable off` made explicit	**Resolved**

Clickjacking	`X-Frame-Options: SAMEORIGIN`	**Resolved**
Missing HttpOnly flag / missing Secure flag on cookies	HttpOnly on the session cookie, Secure on every cookie set over HTTPS, `session.use_strict_mode` enabled	**Resolved**
Server version disclosure (Server header, X-Powered-By, ETag)	`ServerTokens Prod`, `ServerSignature Off`, `expose_php Off`, `FileETag None`, `X-Content-Type-Options`, `Referrer-Policy`	**Resolved**
SSRF surface through PHP remote wrappers (related to CVE-2020-7071, CVE-2021-21705)	The web interface never opens URLs: `allow_url_fopen Off`, `allow_url_include Off`, `enable_dl Off`	Mitigated (attack surface removed)

3. Items NOT addressed by this patch (OpenSSL / Apache update required)

The following require an updated OpenSSL or Apache and cannot be addressed by this patch. However, as the notes show, on the QuikStation they either have no attack path or are limited to denial of service (a temporary outage of the web console); none of them leads to an unauthenticated compromise. They are planned to be addressed by a future patch or firmware update. Customers who must nevertheless address them immediately can continue to use the **web-interface disable scripts from the November 2023 "Security Patch Instructions" bulletin (**`QS-security-patch.sh` **/** `webinterface.sh`**)**. (The bulletin: https://pub-4f6f0f4e63894238a2e6d96abbaa1645.r2.dev/RDX_QuikStation_Security_Patch_Information_and_Instructions_2023-11.pdf; the scripts (QS-Patch.tar): https://pub-4f6f0f4e63894238a2e6d96abbaa1645.r2.dev/QS-Patch.tar. The Overland-Tandberg download location printed in that bulletin is no longer reachable, so the same files are hosted here.) With the web interface stopped, the items below (and those in section 2) are not reachable. Enable the interface temporarily with `webinterface.sh enable` only while configuring the unit, and disable it again afterwards.

Key to the notes: (a) = the vulnerable code is not running / there is no attack path; (b) = applies, but the impact is limited to denial of service or similar; (c) = applies only with a configuration the QuikStation does not have (reverse proxy etc.)

Item	Notes
OpenSSL: CVE-2020-1971, CVE-2021-3449 (mitigated only), CVE-2021-3711, CVE-2021-3712, CVE-2021-	Fixed in OpenSSL 1.1.1w and later. (a) CVE-2022-1292 / 2022-2068 (c_rehash script), 2021-4160 (MIPS only), 2022-2097 (32-bit x86 only) and 2021-3711 (SM2) do not apply. (a) The certificate-parsing issues

4160, CVE-2021-23840, CVE-2021-23841, CVE-2022-0778, CVE-2022-1292, CVE-2022-2068, CVE-2022-2097, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286	CVE-2020-1971, 2021-3712, 2021-23841, 2022-0778, 2022-4450, 2023-0215 and 2023-0286 are not reachable: the unit never receives an attacker-supplied certificate (no client-certificate authentication). (a) CVE-2022-4304 (RSA key exchange) is not reachable after this patch restricts the cipher suites. (b) CVE-2021-23840 is an integer overflow on very large inputs with minor impact
Apache HTTP Server: CVE-2021-34798, CVE-2023-38709, CVE-2024-42516, CVE-2024-38476 and other core fixes	Fixed in Apache 2.4.6x. (a) CVEs in mod_proxy, mod_http2, mod_lua, mod_dav and CGI do not apply (modules not loaded); mod_rewrite CVEs do not apply (no rewrite rules). (b) CVE-2021-34798 crashes a worker process with a crafted header - denial of service, the worker is restarted. (c) CVE-2022-22720 requires a reverse proxy in front of the unit; CVE-2023-38709 / 2024-24795 / 2024-38476 / 2024-42516 require an application that reflects user input into response headers, which the web console does not do
Self-signed TLS/SSL certificate, certificate Subject CN mismatch, untrusted certificate	The unit uses a device-specific self-signed certificate. A man-in-the-middle on the same network remains possible; address it by restricting web-console access to management workstations
ICMP timestamp response	Not addressed, as in the 2023 bulletin
TCP timestamp response	Deliberately left enabled: TCP timestamps (PAWS) are needed for reliable high-speed (10 GbE) iSCSI transfers

4. Firmware updates and the order of applying the patch

Firmware 3.3.0.5 is included in this patch, and **the firmware update needed for the PHP fix is performed by the patch itself**. Only units on firmware 1.x (1.5.1.26 or earlier) need a manual firmware update. The flow by current firmware:

Current firmware	Flow
3.3.0.5	Apply the patch as it is. If the other boot area still holds a firmware older than 3.3.0.5, the patch applies the PHP fix and the mitigation, writes 3.3.0.5 there as well (the unit reboots; a few minutes, up to about 10) and, once the unit is back, installs the PHP fix in both boot areas.
2.5.2–3.2.x	Apply the patch as it is. The Windows / macOS / Linux tools carry out the whole sequence by themselves: mitigation → update to 3.3.0.5 (the unit reboots; a few minutes, up to about 10) → PHP fix → 3.3.0.5 into the other boot area (second reboot) → PHP fix in both boot areas. (If the patch is run directly on the unit, run it again after each reboot.) **Backups and iSCSI connections are interrupted during the reboots, so run the patch when no backup is active.** Updating to 3.3.0.5 by hand first and then applying the patch is fine too.
1.5.1.26 or earlier (1.x)	The patch cannot update firmware 1.x to 2.x (a three-step procedure is needed - see the link below). **Apply the patch first** so the unit is protected by the mitigation, then update to 2.5.2 or later following the procedure below. **That update removes the patch completely, so run the patch again afterwards**; the re-run then performs the update to 3.3.0.5 and the PHP fix automatically.

Details of the three-step update from firmware 1.x: https://drive.google.com/file/d/1C4yG0U92Van-UYk4u5ptwxw-rBgTesYe/view?usp=drive_link

Firmware 3.3.0.5 is included in the patch. If you need it on its own: https://overlandtandberg.co.jp/downloads

If the firmware is updated, re-flashed or downgraded again in the future, **run the patch once more afterwards**. An update between 2.x / 3.x versions leaves the mitigation active, but the PHP fix disappears from the rewritten boot area (a firmware update rewrites that boot area completely). From its third edition the patch keeps a stored copy of the fixed PHP on the unit and, at the next boot, installs the fix again by itself when the rewritten boot area holds the stock PHP of a supported firmware (2.8.0.8 - 3.3.0.5); to be certain, re-run the patch after any update anyway (seconds to a few minutes; this also repairs the mitigation's copies). The state can be seen from the `_phpsec` marker described in section 8. The patch (`qs-patch.sh`) detects the firmware state automatically, so the same

files and the same procedure apply from any starting state.

5. Preparation (all platforms)

1. Log in to the QuikStation web console, open **System Settings > Options > Diagnostics** and enable **Allow Remote Access (SSH)**.
2. On the same tab, **download the key file** (each unit has its own key).
3. Download the patch package and extract it into one folder.
   Download: https://pub-4f6f0f4e63894238a2e6d96abbaa1645.r2.dev/QS-SecurityFix-2026-10-v13.zip
   (file name: `QS-SecurityFix-2026-10-v13.zip`; about 100 MB; the SHA-256 checksums `SHA256SUMS.txt` and this bulletin as PDF are at https://quikstation-patch.pages.dev/)

6. Applying the patch — Windows (one click)

1. Save the key file from section 5 into the extracted folder (it contains `QS-SecurityFix.bat`, `qs-patch.sh`, `qs-secfix.sh`, `qs-phpfix.sh`, `libphp7.so`, `php`, `quikstation_3.3.0.5.swu`, `plink.exe`, `pscp.exe`, `qs-keyconv.ps1`). The file name does not matter.
2. **Double-click** `QS-SecurityFix.bat`. The key file is found automatically.
3. Enter the QuikStation's IP address (the address used for the web console) and press Enter.
4. After the current state is shown, type `YES` at `Type YES to apply the patch:`.
5. The run ends with `RESULT: PROTECTED`. (Do not forget to disable SSH again in step 6 below.) On 1.x units and on units whose both boot areas already run 3.3.0.5 the tool reboots the unit once after applying and confirms `PERSIST: VERIFIED` when it is back. On units that need a firmware update (2.5.2–3.2.x, or 3.3.0.5 with an older firmware in the other boot area) the run includes writing 3.3.0.5 and a reboot (normally two on 2.5.2–3.2.x; a few minutes each, up to about 10 on some models); the tool confirms that the unit went down and came back, then continues by itself. Do not use the unit's web console while the tool runs. **Backups and iSCSI connections are interrupted during the reboot, so run the patch when no backup is active.** On 1.x only the mitigation is applied; the run ends with `RESULT: MITIGATED` and a note. A transcript is saved as `QS-SecurityFix-log.txt` in the same folder.
6. **Finally, be sure to disable SSH again in the web console (System Settings > Options >**

Diagnostics > Allow Remote Access (SSH) off), and delete the downloaded key file.

> Check only: QS-SecurityFix.bat <address> /STATUS Undo: QS-SecurityFix.bat <address> /RESTORE
> Works on Windows 7 and later. Nothing is installed on the PC and the registry is not changed. For several units, place all key files in the folder; the tool asks which unit you mean.

7. Applying the patch — macOS / Linux

Uses the standard OpenSSH client (`ssh`, `scp`, `ssh-keygen`). The included `qs-patch-apply.sh` is the easiest way. It checks the host key presented by the unit against the key file from section 5 and stops if they differ, and it waits for the reboots of a firmware update by itself:

```
chmod +x qs-patch-apply.sh
./qs-patch-apply.sh <address> <key-file>              # apply
./qs-patch-apply.sh <address> <key-file> --status     # check only
./qs-patch-apply.sh <address> <key-file> --restore    # undo
```

Finally, do not forget to disable SSH again in the web console.

Manually:

```
# with a recent OpenSSH add -O to scp (the unit has no SFTP)
chmod 600 <key-file>
ssh -i <key-file> vtx@<address> "mkdir -p /tmp/qsfix"
scp -O -i <key-file> qs-patch.sh qs-secfix.sh qs-phpfix.sh libphp7.so php
vtx@<address>:/tmp/qsfix/
scp -O -i <key-file> quikstation_3.3.0.5.swu vtx@<address>:/srv/www/tmp/   # only if a
firmware update is needed
ssh -t -i <key-file> vtx@<address> "sh /tmp/qsfix/qs-patch.sh"          # answer yes
ssh -i <key-file> vtx@<address> "sh /tmp/qsfix/qs-patch.sh --status"
```

When done manually: if the firmware update reboots the unit, repeat the copy and the run after it is back (until it reports `RESULT: PROTECTED`, or `RESULT: MITIGATED` on 1.x). Only units whose `--status` output has a `PLAN:` line starting with `FWUPDATE` need `quikstation_3.3.0.5.swu` copied.

Finally, do not forget to disable SSH again in the web console.

8. After applying

- Confirm that `--status` (`/STATUS` on Windows) reports `RESULT: PROTECTED` (`RESULT: MITIGATED` on 1.x).
- On a unit running the fixed PHP, the firmware version shown by the web console (About dialog, version field of the system page) carries the suffix `_phpsec` (for example `03.003.00.5_phpsec`). Use it as a quick check of the patch state without the tool. The suffix

is shown only while the fixed PHP is running; it disappears by itself when the fix is gone (after a firmware update, or after `--restore`).

- The web console restarts for a few seconds during the patch; log in again if you were logged in. **Except during the reboot of a firmware update, backups, iSCSI and the network are not affected.**
- After the patch, connecting to the web console requires **TLS 1.2 or later** (TLS 1.2 and 1.3 on firmware 2.x/3.x, TLS 1.2 only on 1.x) (browsers limited to TLS 1.0/1.1 can no longer connect). Windows 8.1 / Server 2012 R2 and later, and current Chrome, Edge, Firefox and Safari are fine.
- If the changed configuration prevented the web server from starting, the patch **rolls itself back automatically** and says so. If the web server cannot start with the fixed PHP, the patch likewise puts the original PHP back (only what this run replaced); the boot hook does the same when the module cannot be loaded and reports it in `--status`. The original PHP is kept on the unit; `--restore` puts it back.
- The patch survives reboots. For firmware updates see section 4. Run the patch once more after any firmware update (within the supported firmware range the PHP fix is re-installed at boot by itself, but the re-run makes it certain).
- The QuikStation 8 runs its system from a copy in RAM made at boot, so the patch updates both the boot area on disk and the running copy in RAM. In the rare case that the RAM copy cannot be updated, the patch reports `RESULT: INSTALLED - RESTART THE UNIT`: restart the unit from the web console, then run the patch again.
- If a firmware update is in progress (accepted but the unit has not rebooted yet) when the patch is run, it changes nothing and reports `RESULT: FIRMWARE UPDATE IN PROGRESS`. Run it again after the reboot. An update can take up to about 15 minutes; do not re-run during that time.
- On a unit whose internal storage has become read-only (rare; settings and logs vanish after a reboot) the patch reports `RESULT: STORAGE FAULT` and does not start the firmware update that would reboot the unit. The mitigation and the PHP fix stay active until the next reboot. If you see this, send the tool's log file and the logs downloaded from the web console to support.
- When finished, disable SSH again in the web console and **delete the downloaded key file** (it gives administrative login to the unit).
- To undo, run `--restore` (`/RESTORE` on Windows).

©2026 Tandberg Data

First edition 20261023 Second edition 20261026
Third edition 20261028