

RDX QuikStation Security Patch 2026-10

Information and Instructions (QuikStation 4 / QuikStation 8)

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. The patch consists of **configuration changes only**: no firmware update and no reboot are involved. It is applied over SSH; the web management interface restarts for a few seconds. **Backup operation, iSCSI connections and the network link are not affected.**

Applies to: every QuikStation 4 / QuikStation 8 / QuikStation8_10G in the field — firmware 1.x (1.3.6–1.5.1.26), 2.x and 3.x. There is no serial-number condition. The patch detects the firmware generation: on 1.x it writes to the single root filesystem and uses a TLS profile valid for OpenSSL 1.0.2 (TLS 1.2 only).

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 applies the mitigations published by the PHP project (`memory_limit=-1`, `session.upload_progress.enabled=0`) and bounds the size of request bodies.

All attack techniques published or observed in the wild as of 22 October 2026 rely on the code paths that these mitigations disable, and do not succeed against a patched unit.

Important: this is an interim measure based on the mitigations published by the PHP project, which the PHP project itself describes as temporary and partial. The complete fix is planned to be delivered, once a fixed PHP is released, either as a patch or as a firmware update. Until then, in addition to this patch, we strongly recommend **restricting access to the web management interface (TCP 80/443) to management workstations or a management network.**

2. Items addressed by this patch

Legend: **Resolved** = finding removed by configuration / Mitigated = exploitation conditions removed or impact limited (a software update is required for the root fix)

Item / CVE	What the patch does	Status
------------	---------------------	--------

CVE-2026-109618 PHP memory corruption during out-of-memory handling (RCE)	PHP memory_limit = -1 (PHP-project mitigation); Apache LimitRequestBody bounds request bodies	Mitigated (emergency)
CVE-2026-109619 PHP use-after-free via state retained between requests (RCE)	PHP session.upload_progress.enabled = 0 (PHP-project mitigation)	Mitigated (emergency)
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: <code>allow_url_fopen</code> Off, <code>allow_url_include</code> Off, <code>enable_dl</code> Off	Mitigated (attack surface removed)
---	--	------------------------------------

3. Items NOT addressed by this patch (software update required)

The following require an updated PHP, OpenSSL or Apache and cannot be addressed by configuration. 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** (`security-patch.sh` / `webinterface.sh`). 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
Obsolete version of PHP (PHP 7.4 series; 7.4.5 on 3.3.0.5)	PHP 7.4 reached end of life in November 2022. A patched PHP will be delivered as a patch or a firmware update
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 and later. (a) CVE-2021-21702 (SOAP), 21703 (FPM), 21704 (Firebird), 2022-31625 (pgsql), 31626 (mysqlnd) and 31630 (GD) do not apply: the QuikStation does not load those extensions. (b) CVE-2019-11048 (disk exhaustion through upload temporary files) is limited to denial of service. (c) The remaining ones concern functions the web console does not use, or have minor impact
OpenSSL: CVE-2020-1971, CVE-2021-3449 (mitigated only), CVE-2021-3711, CVE-2021-3712, CVE-2021-4160, CVE-2021-23840, CVE-2021-23841, CVE-2022-0778, CVE-2022-1292, CVE-2022-2068, CVE-2022-	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 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)

2097, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286	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

How the patch and a firmware update interact depends on the firmware currently installed. **An update from firmware 1.x to 2.x or later removes the patch completely:** the unit is simply back in the "not patched" state (it works normally). **An update between 2.x / 3.x versions leaves the patch active** (the settings live in an area the update does not rewrite and are re-applied to the new firmware's configuration at boot; verified on a QuikStation 4 with the sequence 3.3.0.5 → 3.2.2.5 → 3.3.0.5). The boot area that the update rewrote does lose its own copy of the patch, so **run the patch once more after the update** (it takes a few seconds). Customers who plan to update their firmware are advised to **update to the final firmware 3.3.0.5 first and apply the patch afterwards**.

Current firmware	Recommended order
2.5.2 or later (2.x / 3.x)	Updating to 3.3.0.5 is a single step. Update to 3.3.0.5 first, then apply this patch. If the patch was applied before the update it stays active, but run it once more afterwards and confirm RESULT: PROTECTED. If no firmware update is planned, apply the patch to the current firmware.
1.5.1.26 or earlier (1.x)	Updating firmware 1.x to 3.3.0.5 is a three-step procedure (see the link below this table for the details). Because this takes time, apply the patch to the current firmware first so the unit is protected now. The patch is removed when the unit is updated to 2.5.2 or later, so apply it again after that update. If the three steps are done in one session, one re-application after reaching 3.3.0.5 is enough. If the updates are spread over several days, run <code>--status</code> after each update and re-apply when it reports NOT INSTALLED.

Firmware 3.3.0.5 can be downloaded here: <https://overlandtandberg.co.jp/downloads>

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

In every case the same file and the same procedure are used before and after the update: `qs-secfix.sh` detects the firmware generation automatically.

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://quikstation-patch.pages.dev/QS-SecurityFix-2026-10.zip>

(file name: QS-SecurityFix-2026-10.zip; the SHA-256 checksums SHA256SUMS.txt and this bulletin as PDF are in the same place)

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-secfix.sh, 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. A transcript is saved as QS-SecurityFix-log.txt in the same folder.

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). The included qs-secfix-apply.sh is the easiest way:

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

Manually:

```
chmod 600 <key-file>
scp -i <key-file> qs-secfix.sh vtx@<address>:/tmp/
ssh -i <key-file> vtx@<address> "sh /tmp/qs-secfix.sh"           # answer yes
ssh -i <key-file> vtx@<address> "sh /tmp/qs-secfix.sh --status"
```

8. After applying

- Confirm that --status (/STATUS on Windows) reports RESULT: PROTECTED.
- The web console restarts for a few seconds during the patch; log in again if you were logged in. **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.
- The patch survives reboots (on 2.x/3.x it is stored in both firmware areas). For firmware updates see section 4 (removed by a 1.x → 2.x update, kept by a 2.x/3.x update). After any firmware update, run `--status` and run the patch once more.
- When finished, disable SSH again in the web console.
- To undo, run `--restore` (/RESTORE on Windows).