

RDX QuikStation セキュリティパッチ 2026-10

ご案内と適用手順（QuikStation 4 / QuikStation 8 共通）

1. はじめに

本書は、RDX QuikStation 4 および QuikStation 8/QuikStation8_10G の Web 管理画面（Apache / PHP）に関するセキュリティパッチのご案内です。本パッチは**設定変更のみ**で構成されており、ファームウェアの更新や装置の再起動を伴いません。SSH 経由で適用し、適用後は装置の Web 管理画面が数秒間再起動します。**バックアップ動作・iSCSI 接続・ネットワークリンクには影響しません。**

対象：市場で稼働する全ての QuikStation 4 / QuikStation 8 / QuikStation8_10G。ファームウェア 1.x 系（1.3.6～1.5.1.26）、2.x 系、3.x 系のいずれにも適用できます。特定号機以降などの条件はありません。パッチは適用先のファームウェア世代を自動判別し、1.x 系では単一のルートファイルシステムに書き込み、OpenSSL 1.0.2 の範囲で有効な TLS 設定（TLS 1.2 のみ）を使用します。

緊急対策：PHP の脆弱性「php2shell」（CVE-2026-109618、CVE-2026-109619／CVSS 9.2）

2026 年 10 月 21 日に公開された PHP の重大な脆弱性です。認証不要で、Web 管理画面の任意の URL に細工した HTTP リクエストを 1 回送るだけで、Web サーバー権限での任意コード実行につながります。QuikStation の Web 管理画面は Apache の mod_php で動作しているため該当します。本パッチは、PHP プロジェクト公表の緩和設定（memory_limit=-1、session.upload_progress.enabled=0）とリクエスト本文サイズの上限を設定します。

2026 年 10 月 22 日時点で公開・観測されている攻撃手法は、いずれも上記の緩和設定で無効化される経路を用いており、本パッチを適用した装置では成立しません。

重要：これは PHP プロジェクトが公表している緩和設定に基づく暫定対策であり、PHP プロジェクト自身も「一時的・部分的な緩和」と位置付けています。完全な修正は、修正済み PHP がリリースされた段階で、パッチまたはファームウェア更新の形で提供することを予定しています。それまでの間、本パッチの適用に加えて、**Web 管理画面（TCP 80／443）へのアクセスを管理用端末・管理用ネットワークに限定すること**を強く推奨します。

2. 本パッチで対処する項目

凡例： **解消**＝設定変更により指摘が解消／緩和＝攻撃の成立条件を除去または影響を限定（根本修正はソフトウェア更新が必要）

項目／CVE	本パッチの内容	区分
CVE-2026-109618 PHP メモリ不足処理時のメモリ破壊（RCE）	PHP <code>memory_limit = -1</code> （PHP プロジェクト公表の緩和設定）、Apache <code>LimitRequestBody</code> によるリクエスト本文上限	緩和(緊急)
CVE-2026-109619 PHP リクエスト間の状態保持による use-after-free（RCE）	PHP <code>session.upload_progress.enabled = 0</code> （PHP プロジェクト公表の緩和設定）	緩和(緊急)
CVE-2024-40725 / CVE-2024-39884 Apache：AddType によるハンドラ設定でのソース開示	PHP ハンドラを <code>AddType</code> から <code>SetHandler</code> （ <code>FilesMatch</code> ）方式に変更	解消
CVE-2026-79768 Apache <code>mod_userdir</code> 情報開示	未使用の <code>mod_userdir</code> を無効化	解消
CVE-2026-33007 Apache <code>mod_authn_socache</code> クラッシュ	未使用の <code>mod_authn_socache</code> を無効化	解消
CVE-2021-3449 OpenSSL TLS 再ネゴシエーション時の NULL 参照（DoS）	TLS 1.2 以下の再ネゴシエーションを無効化（ <code>NoRenegotiation</code> ）。※ファームウェア 1.x（OpenSSL 1.0.2）はこの脆弱性の対象外	緩和
CVE-2012-4929 CRIME（TLS 圧縮）	<code>SSLCompression off</code> を明示	解消
TLS 1.0 / TLS 1.1 のサポート（RFC 8996）	TLS 1.2 および 1.3 のみ許可	解消
BEAST（CVE-2011-3389）、Lucky13（CVE-2013-0169）、SWEET32（CVE-2016-2183）、Logjam／一般的な素数の使用（CVE-2015-4000）、静的鍵交換（RSA）暗号、弱い MAC（SHA-1）暗号スイート、	暗号スイートを ECDHE+AEAD（AES-GCM／ChaCha20）のみに限定、サーバー側優先順位を強制、セッションチケット無効化	解消

DES/IDEA 暗号スイート、強い暗号の欠如		
Slowloris 型の低速リクエスト攻撃 (CVE-2007-6750)	RequestReadTimeout を設定	緩和
Cross-Site Tracing (TRACE メソッド)	TraceEnable off を明示	解消
クリックジャッキング	X-Frame-Options: SAMEORIGIN を付与	解消
Cookie の HttpOnly フラグ欠如／Secure フラグ欠如	セッション Cookie に HttpOnly、HTTPS 応答の全 Cookie に Secure を付与、session.use_strict_mode 有効化	解消
サーバーバージョン情報の開示 (Server ヘッダ、X-Powered-By、ETag)	ServerTokens Prod、ServerSignature Off、expose_php Off、FileETag None、X-Content-Type-Options、Referrer-Policy	解消
PHP リモートラッパー経由の SSRF 面 (CVE-2020-7071、CVE-2021-21705 関連)	Web 管理画面は URL を開かないため allow_url_fopen Off、allow_url_include Off、enable_dl Off	緩和(攻撃面の除去)

3. 本パッチの対応外の項目（ソフトウェア更新が必要なもの）

以下は PHP/OpenSSL/Apache 自体の更新が必要であり、本パッチ（設定変更）では対処できません。ただし備考欄に記載のとおり、QuikStation においては攻撃経路が存在しないか、影響が DoS（Web 管理画面の一時的な応答停止）程度にとどまり、認証不要の侵入につながるものではありません。これらは今後、パッチまたはファームウェア更新の形で対処する予定です。それでもこれらの指摘について直ちに対処が必要なお客様は、従来どおり **2023 年 11 月公開の「Security Patch Instructions」に含まれる Web 管理画面の無効化スクリプト**（`QS-security-patch.sh/webinterface.sh`）をご利用ください。Web 管理画面を停止した状態では、以下の項目（および上記 2 章の項目）は到達不能となります。設定が必要な時だけ `webinterface.sh enable` で一時的に有効化し、作業後に `disable` で停止してください。

備考の区分：（a）＝構成上、脆弱なコードが動作していない／攻撃経路が無い （b）＝該当するが影響

は DoS 等に限定 (c) = 該当するが QuikStation に無い構成 (リバースプロキシ等) が前提

項目	備考
Obsolete Version of PHP (PHP 7.4 系、3.3.0.5 では 7.4.5)	PHP 7.4 系は 2022 年 11 月にサポート終了。修正版 PHP はパッチまたはファームウェア更新で提供予定
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	PHP 7.4.33 以降で修正。(a) CVE-2021-21702 (SOAP)、21703 (FPM)、21704 (Firebird)、2022-31625 (pgsql)、31626 (mysqlnd)、31630 (GD) は QuikStation が該当する拡張を読み込んでいないため該当しません。(b) CVE-2019-11048 (アップロード一時ファイルによるディスク圧迫) は DoS に限られます。(c) その他は該当する関数を管理画面が使用していないか、影響が軽微なものです
OpenSSL : CVE-2020-1971、CVE-2021-3449 (緩和のみ)、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-2022-2097、CVE-2022-4304、CVE-2022-4450、CVE-2023-0215、CVE-2023-0286	OpenSSL 1.1.1w 以降で修正。(a) CVE-2022-1292/2022-2068 (c_rehash スクリプト)、2021-4160 (MIPS のみ)、2022-2097 (32 ビット x86 のみ)、2021-3711 (SM2) は該当しません。(a) 証明書解析に関する CVE-2020-1971、2021-3712、2021-23841、2022-0778、2022-4450、2023-0215、2023-0286 は攻撃者の証明書を受け取る経路 (クライアント証明書認証) が無いため到達しません。(a) CVE-2022-4304 (RSA 鍵交換) は本パッチの暗号スイート制限により到達しません。(b) CVE-2021-23840 は巨大入力時の整数オーバーフローで影響は軽微です
Apache HTTP Server : CVE-2021-34798、CVE-2023-38709、CVE-2024-42516、CVE-2024-38476 ほか core の修正	Apache 2.4.6x 以降で修正。(a) mod_proxy/mod_http2/mod_lua/mod_dav/CGI 系の CVE はモジュールを読み込んでいないため、mod_rewrite 系の CVE は書き換えルールが無いため該当しません。(b) CVE-2021-34798 は細工したヘッダで子プロセスが停止する DoS です (自動再起動)。(c) CVE-2022-22720 はリバースプロキシ配下、CVE-2023-38709/2024-24795/2024-38476/2024-42516 は利用者入力を応答ヘッダに反映するアプリが前提で、管理画面では成立しません
自己署名の TLS/SSL 証明書、証明書の Subject CN 不一致、信頼されない証明	装置固有の自己署名証明書を使用しているため。同一ネットワーク内での中間者攻撃の余地は残るため、管理画面へのアクセスを管理用端末に限定する

書	ことで対処してください
ICMP timestamp response	2023 年の案内と同様、対応外です
TCP timestamp response	TCP タイムスタンプは高速（10GbE）iSCSI 転送の信頼性（PAWS）に必要なため、本パッチでは意図的に無効化していません

4. ファームウェア更新とパッチ適用の順序

本パッチとファームウェア更新の関係は、現在のファームウェアにより異なります。**1.x 系から 2.x 系以降への更新ではパッチは完全に消え**、装置は「未適用」の状態に戻ります（動作に支障はありません）。**2.x / 3.x 系の間の更新ではパッチは有効なまま残ります**（設定は更新で書き換わらない領域に保存され、起動時に新しいファームウェアの設定へ自動的に再適用されます。QuikStation 4 で 3.3.0.5→3.2.2.5→3.3.0.5 の更新を行い確認済み）。ただし更新で書き換わった側の起動領域からはパッチの控えが無くなるため、**更新後に本パッチをもう一度実行すること**を推奨します（数秒で終わります）。ファームウェアの更新を予定されているお客様には、**最終ファームウェア 3.3.0.5 へ更新した上で本パッチを適用すること**を推奨します。

現在のファームウェア	推奨する順序
2.5.2 以降 (2.x 系 / 3.x 系)	3.3.0.5 への更新は 1 回の作業で済みます。 先に 3.3.0.5 へ更新し、その後に本パッチを適用 してください。先にパッチを適用してから更新した場合もパッチは有効なまま残りますが、更新後に本パッチをもう一度実行して RESULT: PROTECTED を確認してください。ファームウェアを更新する予定がない場合は、現在のファームウェアにそのまま適用して構いません。
1.5.1.26 以前 (1.x 系)	1.x 系から 3.3.0.5 への更新は 3 段階の更新作業 が必要です（詳細は本表の下リンク）。更新に時間を要するため、 まず現在のファームウェアに本パッチを適用して保護 してください。 2.5.2 以降へ更新した時点でパッチは消えますので、更新後に本パッチを再適用 してください（3 段階を続けて行う場合は 3.3.0.5 到達後に 1 回で足りません）。更新を日を分けて行う場合は、各更新の後に --status で確認し、 NOT INSTALLED なら再適用してください。

ファームウェア 3.3.0.5 のダウンロードはこちらから：

<https://overlandtandberg.co.jp/downloads>

1.x 系からの更新手順（3 段階）の詳細：

<https://drive.google.com/file/d/1C4yG0U92Van-UYk4u5ptwxw-rBgTesYe/view?usp=sharing>

いずれの場合も、本パッチ（qs-secfix.sh）はファームウェア世代を自動判別するため、更新の前後で同じ

ファイル・同じ手順を使用できます。

5. 適用前の準備（共通）

1. QuikStation の Web 管理画面にログインし、**System Settings > Options > Diagnostics** タブで **Allow Remote Access (SSH)** を有効にします。
2. 同じ画面で**鍵ファイルをダウンロード**します（装置ごとに異なります）。
3. パッチ一式をダウンロードし、1つのフォルダに展開します。

ダウンロード：<https://quikstation-patch.pages.dev/QS-SecurityFix-2026-10.zip>

（ファイル名：QS-SecurityFix-2026-10.zip。同じ場所に SHA-256 チェックサム

SHA256SUMS.txt と本書の PDF も置いてあります）

6. 適用手順 — Windows（クリック1つで完了）

1. 展開したフォルダ（QS-SecurityFix.bat、qs-secfix.sh、plink.exe、pscp.exe、qs-keyconv.ps1 が入っています）に、5章でダウンロードした**鍵ファイルを保存**します。ファイル名はそのままで構いません。
2. QS-SecurityFix.bat を**ダブルクリック**します。鍵ファイルは自動的に検出されます。
3. QuikStation の IP アドレス（Web 管理画面を開く時のアドレス）を入力し、Enter を押します。
4. 現在の状態が表示された後、Type YES to apply the patch: と表示されたら YES と入力します。
5. 最後に RESULT: PROTECTED と表示されれば完了です。実行記録は同じフォルダの QS-SecurityFix-log.txt に保存されます。

確認のみ：QS-SecurityFix.bat <IP アドレス> /STATUS 元に戻す：QS-SecurityFix.bat <IP アドレス> /RESTORE
Windows 7 以降で動作します。PC へのインストールやレジストリの変更は行いません。複数台に適用する場合は、各装置の鍵ファイルを同じフォルダに入れておくと、実行時にどの装置かを選択できます。

7. 適用手順 — macOS／Linux

標準の OpenSSH クライアント（ssh、scp）を使用します。同梱の qs-secfix-apply.sh を使うのが簡単です。

```
chmod +x qs-secfix-apply.sh
./qs-secfix-apply.sh <IP アドレス> <鍵ファイル>          # 適用
./qs-secfix-apply.sh <IP アドレス> <鍵ファイル> --status  # 確認のみ
./qs-secfix-apply.sh <IP アドレス> <鍵ファイル> --restore # 元に戻す
```

手動で行う場合：

```
chmod 600 <鍵ファイル>
scp -i <鍵ファイル> qs-secfix.sh vtx@<IP アドレス>:/tmp/
ssh -i <鍵ファイル> vtx@<IP アドレス> "sh /tmp/qs-secfix.sh"          # yes と入力
ssh -i <鍵ファイル> vtx@<IP アドレス> "sh /tmp/qs-secfix.sh --status"
```

8. 適用後の確認と注意事項

- `--status`（Windows では `/STATUS`）で `RESULT: PROTECTED` と表示されることを確認してください。
- 適用中、Web 管理画面は数秒間再起動します。ログイン中の場合は再度ログインしてください。**バックアップ・iSCSI・ネットワークには影響しません。**
- 適用後、Web 管理画面への接続には **TLS 1.2 以上**が必要です（ファームウェア 2.x/3.x では TLS 1.2 と 1.3、1.x では TLS 1.2 のみ）（TLS 1.0/1.1 のみの古いブラウザからは接続できなくなります）。Windows 8.1／Server 2012 R2 以降の標準ブラウザ、および現行の Chrome／Edge／Firefox／Safari は対応しています。
- 設定変更が Web サーバーの起動に失敗した場合、パッチは**自動的に元の設定へ巻き戻し**、その旨を表示します。
- 本パッチは再起動後も有効です（2.x/3.x では両方のファームウェア領域に保存されます）。ファームウェア更新との関係は 4 章のとおりです（1.x→2.x 以降では消える、2.x/3.x 間では残る）。更新後は必ず `--status` で状態を確認し、本パッチをもう一度実行してください。
- 作業後は Web 管理画面で **SSH を無効**に戻してください。

- 元に戻す場合は `--restore` (Windows では `/RESTORE`) を実行してください。