# QNAP

## QNAP-NAS 脆弱性関連情報ポータル 2026

こちらはQNAP社が公開する
最新のNAS関連の脆弱性情報のうち、影響・危険度が「高/重要
」以上を掲載しています。ご利用いただくNAS内データの消失や漏洩などの損害を防ぐため、こちらのページを定期的にチェックしてください。

尚、発見された脆弱性への基本的な対策はメーカー
が公開する対策済みバージョンのNAS-
OS/アプリケーションへのアップデート
となります。特にLAN外部からのNASへのアクセスを許可、或いは、共有フォルダを外部公開しているといった場合には、各項に記載される対策手段を速やかに実施いただくを強くお勧めします。

※ご注意
・記載される情報はページ公開時点のものとなり、今後記載内容が更新される可能性があります。
・新たな脆弱性関連のニュースの公開に併せて、解決済みの旧い情報から順次削除します。
・リンク先メーカーウェブサイトの脆弱性情報ページ「セキュリティ・アドバイザリー
」の詳細解説は英語のみとなります。内容の確認にあたっては必要に応じてブラウザの翻訳機能等をご利用ください。

---

## ■最新の脆弱性情報 ※2026年 3月23日 更新

### QuRouter の複数の脆弱性

最終更新日：2026年 3月 21日
セキュリティID：QSA-26-12
危険度：**緊要**
CVE-2025-62843,ZDI-CAN-28371,CVE-2025-62844,ZDI-CAN-28422,CVE-2025-62846,ZDI-CAN-28424,CVE-2025-62845,ZDI-CAN-28423
影響を受ける製品：**QuRouter 2.6.x**

QuRouterに複数の脆弱性が複数報告されています。

・CVE-2025-62843: 通信チャネルが本来のエンドポイントにのみ制限されているという脆弱性
撃者が物理的にシステムにアクセスした場合、本来そのエンドポイントに割り当てられていた権限を取得する可能性があります。

・CVE-2025-62844: 脆弱な認証の脆弱性
攻撃者がローカルネットワークへのアクセス権を取得した場合、機密情報を入手する可能性があります。

・CVE-2025-62846: SQLインジェクションの脆弱性
ローカル攻撃者が管理者アカウントを取得した場合、不正なコードやコマンドを実行することが可能になります。

・CVE-2025-62845: エスケープシーケンス、メタシーケンス、または制御シーケンスの不適切な無効化の脆弱性
ローカル攻撃者が管理者アカウントを取得した場合、予期しない動作を引き起こす可能性があります。

ステータス：解決済み
対策手段：
対象となるアプリバージョンを利用している場合に
は、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
| --- | --- |
| QuRouter 2.6.x | QuRouter 2.6.3.009<br>およびそれ以降の各バージョン |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QuRouter (PWN2OWN 2025)

---

**QuNetSwitch の脆弱性**

最終更新日：2026年 3月 21日
セキュリティID：QSA-26-11
危険度：**緊要**
CVE-2026-22897,CVE-2026-22900,CVE-2026-22901,CVE-2026-22902
影響を受ける製品：**QuNetSwitch 2.0.x**

QuNetSwitch に複数の脆弱性が複数報告されています。

・CVE-2026-22897: コマンドインジェクションの脆弱性
リモート攻撃者は任意のコマンドを実行できます。

・CVE-2026-22900: ハードコードされた認証情報の脆弱性
リモート攻撃者が不正アクセスを取得する可能性があります。

・CVE-2026-22901: コマンドインジェクションの脆弱性
リモート攻撃者がユーザーアカウントを取得した場合、任意のコマンドを実行できます。

・CVE-2026-22902: コマンドインジェクションの脆弱性
ローカル攻撃者が管理者アカウントを取得した場合、任意のコマンドを実行できます。

ステータス：解決済み
対策手段：
対象となるアプリバージョンを利用している場合に
は、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QuNetSwitch 2.0.x | QuNetSwitch 2.0.4.0415 およびそれ以降<br>QuNetSwitch 2.0.5.0906 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ： Multiple Vulnerabilities in QuNetSwitch (ADRA NDR)

---

**QVR Pro の脆弱性**

最終更新日：2026年 3月 21日
セキュリティID：QSA-26-7
危険度：**重要**
CVE-2026-22898,ZDI-CAN-28327
影響を受ける製品：**QVR Pro 2.7.x**

QVR

Proに複数の脆弱性が報告されています。
この脆弱性が悪用されると、リモートの攻撃者がシステムへのアクセスを奪取する可能性があります。

・CVE-2026-22898 : 重要な機能に対する認証の欠落

ステータス：解決済み
対策手段：
対象となるアプリバージョンを利用している場合に
は、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QVR Pro 2.7.x | QVR Pro 2.7.4.1815 およびそれ以降の各バージョン |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in QVR Pro

---

**QTS および QuTS hero の複数の脆弱性**

最終更新日：2026年 2月 12日
セキュリティID：QSA-26-5
危険度：**重要**
CVE-2025-47205,CVE-2025-58466,CVE-2025-66277
影響を受ける製品：**QTS 5.2.x, QuTS hero h5.2.x**

QTSおよびQuTS heroに複数の脆弱性が報告されています。

・CVE-2025-58466: 初期化されていない変数脆弱性の利用
リモート攻撃者が管理者アカウントにアクセスした場合、その脆弱性を利用してサービス拒否(DoS)状態を引き起こしたり、予期せぬ方法で制御フローを変更したりすることができます。

・CVE-2025-47205: NULLポインタのデリファレンス脆弱性
リモート攻撃者が管理者アカウントにアクセスした場合、その脆弱性を利用してサービス拒否(DoS)攻撃を開始できます。

・CVE-2025-66277:リンク追従の脆弱性
悪用された場合、リモート攻撃者がファイルシステムを意図しない場所に移動できる可能性があります。

ステータス：解決済み
対策手段：
対象となるファームウェアを利用している場合には、
下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QTS 5.2.x<br>QuTS hero h5.2.x | QTS 5.2.8.3350 build 20251216<br>QuTS hero h5.2.8.3350 build 20251216 |

| |
|---|
| およびそれ以降の各バージョン |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QTS and QuTS hero

---

**File Station 5 の複数の脆弱性**

最終更新日：2026年 2月 12日
セキュリティID：QSA-26-3
危険度：**重要**
CVE識別子:CVE-2025-54155,CVE-2025-54161,CVE-2025-54162,CVE-2025-54163,CVE-2025-54169,CVE-2025-57707,CVE-2025-57713,CVE-2025-62853,CVE-2025-62854,CVE-2025-62855,CVE-2025-62856,CVE-2025-66278,CVE-2026-22894
影響を受ける製品：**File Station 5 バージョン 5.5.x**

File Station 5 に複数の脆弱性が複数報告されています。攻撃者がユーザーアカウントにアクセスした場合、これらの脆弱性を悪用してシステムのセキュリティを侵害する可能性があります。

・CVE-2025-54155,CVE-2025-54161:制限のないリソース割り当てやスロットリングの脆弱性
リモート攻撃者が管理者アカウントにアクセスした場合、その脆弱性を利用して他のシステム、アプリケーション、プロセスが同じ種類のリソースにアクセスするのを防ぐことができます。

・CVE-2025-54162:パストラバーサルの脆弱性
リモート攻撃者が管理者アカウントにアクセスした場合、予期せぬファイルやシステムデータの内容を読み取るために脆弱性を悪用できます。

・CVE-2025-62853,CVE-2025-66278,CVE-2026-22894:パストラバーサルの脆弱性
リモート攻撃者がユーザーアカウントにアクセスした場合、予期せぬファイルやシステムデータの内容を読み取るために脆弱性を悪用できます。

・CVE-2025-62855,CVE-2025-62856:パストラバーサルの脆弱性
ローカル攻撃者が管理者アカウントを入手すると、予期せぬファイルやシステムデータの内容を読み取るために脆弱性を悪用できます。

・CVE-2025-54163: NULLポインタの参照解除
脆弱性 リモート攻撃者が管理者アカウントにアクセスした場合、その脆弱性を利用してサービス拒否(DoS)攻撃を開始できます。

・CVE-2025-54169:境界外読み取りの脆弱性
リモート攻撃者がユーザーアカウントにアクセスした場合、その脆弱性を利用して秘密データを入手できます。

・CVE-2025-57707:静的に保存されたコードにおける指令の不適切な中和(静的コード注入)脆弱性
リモート攻撃者がユーザーアカウントにアクセスした場合、その脆弱性を利用して制限されたデータやファイルにアクセスできます。

・CVE-2025-57713:認証の弱い脆弱性
悪用された場合、リモート攻撃者は機密情報を入手する可能性があります。

・CVE-2025-62854: 制御されていないリソース消費の脆弱性
リモート攻撃者がユーザーアカウントを入手した場合、その脆弱性を利用してサービス拒否(DoS)攻撃を仕掛けることができます。

---

ステータス：解決済み
対策手段：対象となるFile Station 5アプリケーションを利用している場合には、下記の修正/対策

済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| File Station 5 version 5.5.x | File Station 5 version 5.5.6.5190 およびそれ以降の各バージョン |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in File Station 5

---

**Qfiling の脆弱性**

最終更新日：2026年 1月 3日
セキュリティID：QSA-25-54
危険度：**重要**
CVE-2025-59384
影響を受ける製品：**Qfiling 3.13.x**

Qfiling にパストラバーサルの脆弱性が報告されています。
リモートによる攻撃者にこの脆弱性を悪用された場合、予期せずデータファイルやシステムデータの内容等が読み取られる可能性があります。

ステータス：解決済み
対策手段：
対象となるQfilingアプリケーションを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| Qfiling 3.13.x | Qfiling 3.13.1 およびそれ以降の各バージョン |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in Qfiling

---

**MARS (Multi-Application Recovery Service) の脆弱性**

最終更新日：2026年 1月 3日
セキュリティID：QSA-25-53
危険度：**重要**
CVE-2025-59387
影響を受ける製品：**MARS (Multi-Application Recovery Service) 1.2.x**

MARS（Multi-Application Recovery Service）にSQLインジェクションの脆弱性が報告されています。
リモートによる攻撃者にこの脆弱性を悪用された場合、不正なコードやコマンドが実行される可能性があります。

ステータス：解決済み
対策手段：

対象となるMARSアプリケーションを利用し
ている場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| MARS 1.2.x | MARS 1.2.1.1686<br>およびそれ以降の各バージョン |

注:バージョン1.3.x以降、アプリケーション名はHDP for Wordpress(MARS)に変更されました。

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in MARS (Multi-Application Recovery Service)

---

**QuMagie の脆弱性**

最終更新日：2025年 11月 8日
セキュリティID：QSA-25-33
危険度：**重要**
CVE-2025-52425
影響を受ける製品：**QuMagie 2.6.x**

QuMagie にSQLインジェクションの脆弱性が存在することが報告されています。リモートによる攻撃者がこの脆弱性を悪用した場合、不正なコードやコマンドが実行される可能性があります。

ステータス：解決済み
対策手段：
対象となるQuMagieを利用している場合には、下記の修正/対策
済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QuMagie 2.6.x | QuMagie 2.7.0<br>およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in QuMagie

**QuMagie の脆弱性 2**

最終更新日：2025年 11月 8日
セキュリティID：QSA-25-43
危険度：**重要**
CVE-2025-58464
影響を受ける製品：**QuMagie 2.7.x**

QuMagie に相対パス・トラバーサル脆弱性が報告されています。リモートによる攻撃者がこの脆弱性を悪用した場合、予期しないファイルやシステムデータのコンテンツを読み取ることが可能になります。

ステータス：解決済み
対策手段：

対象となるQuMagieを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QuMagie 2.7.x | QuMagie 2.7.3 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in QuMagie

---

**Hyper Data Protector の脆弱性**

最終更新日：2025年 11月 8日
セキュリティID：QSA-25-48
危険度：重要
CVE-2025-59389
影響を受ける製品：**Hyper Data Protector 2.2.x**

Hyper Data Protector 2.2.x に脆弱性が報告されています。

ステータス：解決済み
対策手段：対象となるHyper Data Protectorを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| Hyper Data Protector 2.2.x | Hyper Data Protector 2.2.4.1 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in Hyper Data Protector (PWN2OWN 2025)

---

**Malware Remover の脆弱性**

最終更新日：2025年 11月 8日
セキュリティID：QSA-25-47
危険度：重要
CVE-2025-11837,ZDI-CAN-28324
影響を受ける製品：**Malware Remover 6.6.x**

Malware Remover に脆弱性が報告されています。

ステータス：解決済み
対策手段：対象となるMalware Removerを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
| --- | --- |
| Malware Remover 6.6.x | Malware Remover 6.6.8.20251023 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in Malware Remover (PWN2OWN 2025)

---

**HBS 3 の脆弱性**

最終更新日：2025年 11月 8日
セキュリティID：QSA-25-46
危険度：重要
CVE-2025-62840,CVE-2025-62842,ZDI-CAN-28426,ZDI-CAN-28428
影響を受ける製品：**HBS 3 Hybrid Backup Sync 26.1.x 以前**

HBS 3 Hybrid Backup Sync に複数の脆弱性が報告されています。

ステータス：解決済み
対策手段：対象となるHBS 3を利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
| --- | --- |
| HBS 3 Hybrid Backup Sync 26.1.x およびそれ以前 | HBS 3 Hybrid Backup Sync26.2.0.938 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in HBS 3 Hybrid Backup Sync (PWN2ONW 2025)

---

**QTSおよびQuTS hero の脆弱性**

最終更新日：2025年 11月 8日
セキュリティID：QSA-25-45
危険度：重要
CVE識別子:CVE-2025-62847,CVE-2025-62848,CVE-2025-62849,ZDI-CAN-28353,ZDI-CAN-28435,ZDI-CAN-28436
影響を受ける製品：**QTS 5.2.x, QuTS hero h5.2.x, QuTS hero h5.3.x**

QTS、およびQuTS hero に複数の脆弱性が報告されています。

ステータス：解決済み
対策手段：対象となるQTS/QuTS heroを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
| --- | --- |

| | |
|---|---|
| QTS 5.2.x | QTS 5.2.7.3297 build 20251024 およびそれ以降 |
| QuTS hero h5.2.x | QuTS hero h5.2.7.3297 build 20251024 およびそれ以降 |
| QuTS hero h5.3.x | QuTS hero h5.3.1.3292 build 20251024 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QTS and QuTS hero (PWN2OWN 2025)

---

**Qsync Central の脆弱性**

最終更新日：2025年 11月 8日
セキュリティID：QSA-25-41
危険度：**重要**
CVE-2025-57712
影響を受ける製品：**Qsync Central 5.0.x**

Qsync Central にパス・トラバーサル脆弱性が報告されています。リモートによる攻撃者がユーザーアカウントにアクセスした場合、この脆弱性を悪用して予期しないファイルやシステムデータのコンテンツを読み取ることが可能になります。

ステータス：解決済み
対策手段：対象となるQsync Centralを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| Qsync Central 5.0.x | Qsync Central 5.0.0.3(2025/08/28) およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in Qsync Central

---

**Download Station の複数の脆弱性**

最終更新日：2025年 11月 8日
セキュリティID：QSA-25-37
危険度：**重要**
CVE-2025-58463, CVE-2025-58465
影響を受ける製品：**Download Station 5.10.x** (QTS, 及び QuTS hero用)

Download Station に複数の脆弱性が報告されています。

CVE-2025-58463: 相対パス・トラバーサル脆弱性
リモートの攻撃者が管理者アカウントへのアクセス権を取得した場合、この脆弱性を悪用して、意図しないファイ

ルやシステムデータのコンテンツを読み取ることができます。
CVE-2025-58465: クロスサイトスクリプティング（XSS）脆弱性
リモートの攻撃者がユーザーアカウントへのアクセス権を取得した場合、この脆弱性を悪用してセキュリティメカニズムを回避したり、アプリケーションデータを読み取ったりすることができます。

ステータス：解決済み
対策手段：対象となるDownload Stationを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| Download Station 5.10.x (for QTS 5.2.1) | Download Station 5.10.0.305(2025/09/16) およびそれ以降 |
| Download Station 5.10.x (for QuTS hero h5.2.1) | Download Station 5.10.0.304(2025/09/08) およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in Download Station

---

**NetBak Replicator の脆弱性**

最終更新日：2025年 10月 4日
セキュリティID：QSA-25-39
危険度：**重要**
CVE識別子:CVE-2025-57714
影響を受ける製品：**NetBak Replicator 4.5.x**

NetBak Replicator に、引用符で囲まれていない検索パスまたは要素の脆弱性が報告されています。ローカルの攻撃者がユーザーアカウントにアクセスした場合、この脆弱性を悪用して不正なコードやコマンドを実行する可能性があります。

ステータス：解決済み
対策手段：対象となるNetBak Replicatorを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| NetBak Replicator 4.5.x | NetBak Replicator 4.5.15.0807 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in NetBak Replicator

---

**Qsync Central アプリ の脆弱性**

最終更新日：2025年 10月 4日
セキュリティID：QSA-25-35

危険度：**重要**
CVE識別子:CVE-2025-44012 ¦ CVE-2025-47210 ¦ CVE-2025-52867 ¦ CVE-2025-53595 ¦ CVE-2025-54153
影響を受ける製品：**Qsync Central 5.0.0**

Qsync Central に、複数の脆弱性が報告されています。

CVE-2025-44012: リモートの攻撃者がユーザー アカウントにアクセスした場合、その脆弱性を悪用して、他のシステム、アプリケーション、またはプロセスが同じ種類のリソースにアクセスできないようにすることができます。
CVE-2025-47210: リモートの攻撃者がユーザー
アカウントにアクセスした場合、その脆弱性を悪用してサービス拒否 (DoS) 攻撃を開始する可能性があります。
CVE-2025-52867: リモートの攻撃者がユーザー
アカウントにアクセスした場合、その脆弱性を悪用してサービス拒否 (DoS) 攻撃を開始する可能性があります。
CVE-2025-53595, CVE-2025-54153: リモートの攻撃者がユーザー
アカウントにアクセスした場合、脆弱性を悪用して不正なコードやコマンドを実行する可能性があります。

ステータス：解決済み
対策手段：対象となるQsync Centralを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| Qsync Central 5.0.0 | Qsync Central 5.0.0.2 (2025/07/31) およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in Qsync Central

---

**Video Stationアプリ の脆弱性**

最終更新日：2025年 10月 4日
セキュリティID：QSA-25-32
危険度：**重要**
CVE識別子:CVE-2024-56804
影響を受ける製品：**Video Station 5.8.x**

QNAP純正アプリケーション Video Station にSQLインジェクションの脆弱性が報告されています。リモート攻撃者がユーザーアカウントにアクセスした場合、この脆弱性を悪用して不正なコードやコマンドを実行する可能性があります。

ステータス：解決済み
対策手段：
対象となるアプリケーションソフトを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| Video Station 5.8.x | Video Station 5.8.4 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用くださ

い。

詳細・対策実施手順掲載ページ：Vulnerability in Video Station

---

**License Centerアプリ の脆弱性**

最終更新日：2025年 8月 29日
セキュリティID：QSA-25-27
危険度：**重要**
CVE識別子:CVE-2025-22483
影響を受ける製品：**License Center 1.8.x, 1.9.x**

QNAP純正アプリケーション ライセンスセンター
にクロスサイトスクリプティング（XSS）の脆弱性が報告されています。
リモート攻撃者が管理者アカウントにアクセスした場合、この脆弱性を悪用してセキュリティメカニズムを回避したり、アプリケーションデータを読み取ったりすることが可能です。

ステータス：解決済み
対策手段：
対象となるアプリケーションソフトを利用し
ている場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| License Center 1.8.x | License Center 1.8.51 およびそれ以降 |
| License Center 1.9.x | License Center 1.9.51 and later およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in License Center

---

**Qsync Central の脆弱性**

最終更新日：2025年 8月 29日
セキュリティID：QSA-25-22
危険度：**重要**
CVE識別子:CVE-2025-29893 ¦ CVE-2025-29894 ¦ CVE-2025-29898 ¦ CVE-2025-30260 ¦ CVE-2025-30275 ¦ CVE-2025-30277 ¦ CVE-2025-30278 ¦ CVE-2025-33033 ¦ CVE-2025-33036 ¦ CVE-2025-33037 ¦ CVE-2025-33038
影響を受ける製品：**Qsync Central 4.5.x**

Qsync Central に複数の脆弱性が報告されています。

CVE-2025-29893, CVE-2025-29894: リモートの攻撃者がユーザー アカウントにアクセスした場合、SQL インジェクションの脆弱性を悪用して不正なコードやコマンドを実行する可能性があります。
CVE-2025-29898: リモートの攻撃者がユーザー
アカウントにアクセスすると、制御されていないリソース消費の脆弱性を悪用して、サービス拒否 (DoS) 攻撃を開始する可能性があります。
CVE-2025-30260: リモート攻撃者がユーザー アカウントにアクセスした場合、制限のないリソースの割り当てやスロットリングの脆弱性を悪用して、他のシステム、アプリケーション、またはプロセスが同じ種類のリソースにアクセスできないようにすることができます。
CVE-2025-30275: リモートの攻撃者がユーザー アカウントにアクセスした場合、NULL ポインタ逆参照の脆弱性を悪用してサービス拒否 (DoS) 攻撃を開始できます。
CVE-2025-30277, CVE-2025-30278: リモートの攻撃者がユーザー アカウントにアクセスした場合、不適切な証明

書検証の脆弱性を悪用してシステムのセキュリティを侵害する可能性があります。
CVE-2025-33033, CVE-2025-33036, CVE-2025-33037, CVE-2025-33038: リモートの攻撃者がユーザーアカウントにアクセスした場合、パス トラバーサルの脆弱性を悪用して予期しないファイルやシステムデータの内容を読み取ることができます。

ステータス：解決済み
対策手段：
対象となるアプリケーションソフトを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| Qsync Central 4.5.x | Qsync Central 4.5.0.7 (2025/04/23) およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in Qsync Central

---

**QuRouter の脆弱性**

最終更新日：2025年 8月 29日
セキュリティID：QSA-25-25
危険度：**重要**
CVE識別子:CVE-2025-29887
影響を受ける製品：**QuRouter 2.5.x**

QuRouterにコマンドインジェクションの脆弱性が報告されています。リモート攻撃者が管理者アカウントにアクセスした場合、この脆弱性を悪用して任意のコマンドを実行する可能性があります。

ステータス：解決済み
対策手段：
対象となるファームウェアバージョンを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QuRouter 2.5.x | QuRouter 2.5.1.060 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in QuRouter

---

**QTSおよびQuTS hero の脆弱性**

最終更新日：2025年 8月 29日
セキュリティID：QSA-25-21
危険度：**重要**
CVE識別子:CVE-2025-29882 ¦ CVE-2025-30264 ¦ CVE-2025-30265 ¦ CVE-2025-30267 ¦ CVE-2025-30268 ¦ CVE-2025-30270 ¦ CVE-2025-30271 ¦ CVE-2025-30272 ¦ CVE-2025-30273 ¦ CVE-2025-30274 ¦ CVE-2025-33032
影響を受ける製品：**QTS 5.2.x, QuTS hero h5.2.x**

# QNAP

QTSおよびQuTS heroに、複数の脆弱性が報告されています。

CVE-2025-29882: リモートの攻撃者がユーザー アカウントにアクセスした場合、NULL ポインタ逆参照の脆弱性を悪用してサービス拒否 (DoS) 攻撃を開始できます。
CVE-2025-30264: リモートの攻撃者がユーザー アカウントにアクセスした場合、コマンド インジェクションの脆弱性を悪用して任意のコマンドを実行する可能性があります。
CVE-2025-30265: リモートの攻撃者がユーザー アカウントにアクセスすると、バッファ オーバーフローの脆弱性を悪用してメモリを変更したり、プロセスをクラッシュさせたりする可能性があります。
CVE-2025-30267, CVE-2025-30268, CVE-2025-30272, CVE-2025-30274: リモートの攻撃者がユーザー アカウントにアクセスした場合、NULL ポインタ逆参照の脆弱性を悪用してサービス拒否 (DoS) 攻撃を開始する可能性があります。
CVE-2025-30270, CVE-2025-30271, CVE-2025-33032: リモートの攻撃者がユーザー アカウントにアクセスした場合、パス トラバーサルの脆弱性を悪用して予期しないファイルやシステム データの内容を読み取ることができます。
CVE-2025-30273: リモートの攻撃者がユーザー アカウントにアクセスした場合、境界外書き込みの脆弱性を悪用してメモリを変更または破壊する可能性があります。

ステータス：解決済み
対策手段：
対象となるファームウェアバージョンを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QTS 5.2.x | QTS 5.2.5.3145 build 20250526 およびそれ以降 |
| QuTS hero h5.2.x | QuTS hero h5.2.5.3138 build 20250519 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QTS and QuTS hero

---

## NAKIVO Backup & Replication の脆弱性

最終更新日：2025年 3月 22日
セキュリティID：QSA-25-08
危険度：**重要**
CVE識別子:CVE-2024-48248
影響を受ける製品：**NAKIVO Backup & Replication 10.11.3.86570 およびそれ以前のバージョン**

NAKIVO Backup & Replicationに脆弱性が発見されました。
この脆弱性により、攻撃者は認証なしで影響を受けるシステム上の任意のファイルを読み取ることができます。この脆弱性が悪用されると、設定ファイル、バックアップ、認証情報などの機密データが漏洩し、データ侵害やさらなるセキュリティ侵害につながる可能性があります。

ステータス：対策中
対策手段：最新のアップデートが利用可能になり次第、すぐにApp Centerにインストールすることをお勧めします。

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in NAKIVO Backup & Replication

---

## File Station 5 の複数の脆弱性

最終更新日：2025年 6月 7日
セキュリティID：QSA-25-16
危険度：**重要**
CVE識別子:CVE-2025-22484,CVE-2025-22490,CVE-2025-29871,CVE-2025-29872,CVE-2025-29873,CVE-2025-29876,CVE-2025-29877,CVE-2025-33035,CVE-2025-30279,CVE-2025-33031
影響を受ける製品：**File Station 5 version 5.5.x**

File Station 5 に不適切な証明書検証の脆弱性が複数報告されています。

CVE-2025-22484, CVE-2025-29872:
制限のないリソース割り当てに関する脆弱性があり、リモート攻撃者がユーザー アカウントにアクセスした場合、他のシステム、アプリケーション、またはプロセスが同じ種類のリソースへのアクセスを阻害ことを可能とします。
CVE-2025-22490, CVE-2025-29873, CVE-2025-29876, CVE-2025-29877:
NULLポインタ参照の脆弱性があり、リモートの攻撃者がユーザー
アカウントにアクセスすると、脆弱性を悪用してサービス拒否 (DoS) 攻撃を開始する可能性があります。
CVE-2025-29871: 境界外読み出しの脆弱性があり、ローカルの攻撃者が管理者アカウントにアクセスした場合、脆弱性を悪用して秘密データを取得する可能性があります。
CVE-2025-33035: パストラバーサルの脆弱性があり、リモートの攻撃者がユーザー
アカウントにアクセスすると、脆弱性を悪用して予期しないファイルやシステム
データの内容を読み取ることができます。
CVE-2025-30279, CVE-2025-33031: 不適切な証明書検証の脆弱性があり、リモートの攻撃者がユーザー
アカウントにアクセスした場合、システムのセキュリティを侵害する可能性があります。

ステータス：解決済み
対策手段：対象となるFile
Stationアプリを利用している場合には、下記の修正/対策
済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| File Station 5<br>version5.5.x | File Station 5 version<br>5.5.6.4847<br>およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in File Station 5

---

## OpenSSH の複数の脆弱性

最終更新日：2025年 6月 7日
セキュリティID：QSA-25-14
危険度：**重要**
CVE識別子:CVE-2025-26465,CVE-2025-26466
影響を受ける製品：**QTS 5.2.x, QuTS hero h5.2.x**

OpenSSHに複数の脆弱性が報告されており、QTS、およびQuTS heroへの影響があります。

ステータス：解決済み
対策手段：対象となるOSを利用している場合には、下記の修正/対策
済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QTS 5.2.x | QTS 5.2.4.3079 build 20250321 およびそれ以降 |
| QuTS hero h5.2.x | QuTS hero h5.2.4.3079 build 20250321 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in OpenSSH

---

**OpenSSH の脆弱性**

最終更新日：2025年 6月 7日
セキュリティID：QSA-25-13
危険度：**重要**
CVE識別子:CVE-2024-6387
影響を受ける製品：**QES 2.2.0**

OpenSSHに脆弱性が報告されており、QESへの影響があります。

ステータス：解決済み
対策手段：
対象となるQES/OSを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QES 2.2.0 | QES 2.2.1 build 20250304 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in OpenSSH

---

**QTSおよびQuTS hero の複数の脆弱性**

最終更新日：2025年 6月 7日
セキュリティID：QSA-25-12
危険度：**重要**
CVE識別子:CVE-2025-22481,CVE-2024-56805
影響を受ける製品：**QTS 5.2.x、QuTS hero h5.2.x**

QTSおよびQuTS heroに、複数の脆弱性が報告されています。

CVE-2025-22481: コマンドインジェクションの脆弱性があり、リモートの攻撃者がユーザーアカウントにアクセスした場合、脆弱性を悪用して任意のコマンドを実行する可能性があります。
CVE-2024-56805: バッファオーバーフローの脆弱性があり、リモートの攻撃者がユーザー アカウントにアクセスした場合、脆弱性を悪用してメモリを変更したりプロセスをクラッシュさせたりする可能性があります。

ステータス：解決済み
対策手段：対象となるOSを利用している場合には、下記の修正/対策

済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QTS 5.2.x | QTS 5.2.4.3079 build 20250321 およびそれ以降 |
| QuTS hero h5.2.x | QuTS hero h5.2.4.3079 build 20250321 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QTS and QuTS hero

---

**Qsync Central の複数の脆弱性**

最終更新日：2025年 6月 7日
セキュリティID：QSA-25-10
危険度：**重要**
CVE識別子:CVE-2025-22482,CVE-2025-29892
影響を受ける製品：**Qsync Central 4.5.x**

Qsync Central に、複数の脆弱性が報告されています。

CVE-2025-22482: 外部制御フォーマット文字列の脆弱性があり、リモートの攻撃者がユーザーアカウントにアクセスした場合、この脆弱性を悪用して機密データを取得したり、メモリを変更したりする可能性があります。
CVE-2025-29892: SQLインジェクションの脆弱性があり、リモートの攻撃者がユーザーアカウントにアクセスした場合、脆弱性を悪用して不正なコードやコマンドを実行する可能性があります。

ステータス：解決済み
対策手段：対象となるQsync Centralアプリを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| Qsync Central 4.5.x | Qsync Central 4.5.0.6 (2025/03/20) およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in Qsync Central

---

**File Station 5 の複数の脆弱性**

最終更新日：2025年 6月 7日
セキュリティID：QSA-25-09
危険度：**重要**
CVE識別子:CVE-2025-22486,CVE-2025-29883,CVE-2025-29884,CVE-2025-29885
影響を受ける製品：**File Station 5 version 5.5.x**

File Station 5
に不適切な証明書検証の脆弱性が複数報告されています

。
リモートの攻撃者がユーザーアカウントにアクセスした場合、これらの脆弱性を悪用してシステムのセキュリティを侵害する可能性があります。

ステータス：解決済み
対策手段：対象となるFile Stationアプリを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| File Station 5 version5.5.x | File Station 5 version 5.5.6.4791 およびそれ以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in File Station 5

---

## ヘルプデスク の脆弱性

最終更新日：2025年 3月 8日
セキュリティID：QSA-25-05
危険度：**重要**
CVE識別子:CVE-2024-50394
影響を受ける製品：Helpdesk 3.3.x

不適切な証明書検証の脆弱性が Helpdesk に影響を及ぼすことが報告されています。この脆弱性が悪用された場合、リモートの攻撃者がシステムのセキュリティを侵害する可能性があります。※Helpdeskが無効になっているシステムには影響しません。

ステータス：解決済み
対策手段：
対象となるHelpdeskを利用している場合には、下記の修正/対策済みバージョンへアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| Helpdesk 3.3.x | Helpdesk 3.3.3 以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in Helpdesk

---

## Rsync に複数の脆弱性

最終更新日：2025年 1月 23日
セキュリティID：QSA-25-02
危険度：**重要**
CVE識別子:
CVE-2024-12084,CVE-2024-12085,CVE-2024-12086,CVE-2024-12087,CVE-2024-12088,CVE-2024-12747
影響を受ける製品：HBS 3 Hybrid Backup Sync 25.1.x

rsyncに複数の脆弱性が報告されています。この脆弱性が悪用されると HBS 3 Hybrid Backup Sync に影響を及ぼします。

ステータス：解決済み
対策手段：対象となるHBSを利用している場合には、下記の修正/対策済みバージョンへアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| HBS 3 Hybrid Backup Sync 25.1.x | HBS 3 Hybrid Backup Sync 25.1.4.952 以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in Rsync

---

**QTS および QuTS hero に複数の脆弱性**

最終更新日：2024年 12月 7日
セキュリティID：QSA-24-49
危険度：**重要**
CVE識別子:CVE-2024-48859,CVE-2024-48865,CVE-2024-48866,CVE-2024-48867,CVE-2024-48868,CVE-2024-50393 ,CVE-2024-50402,CVE-2024-50403
影響を受ける製品：QTS 5.1.x, 5.2.x; QuTS hero h5.1.x, h5.2.x

特定の QNAPオペレーティングシステムバージョンに影響を及ぼす複数の脆弱性が報告されています。

CVE-2024-48859: この脆弱性が悪用された場合、不正認証によりリモートの攻撃者がシステムのセキュリティを侵害する可能性があります。
CVE-2024-48865: この脆弱性が悪用された場合、不正認証によりローカルネットワーク上の攻撃者がシステムのセキュリティを侵害する可能性があります。
CVE-2024-48866: この脆弱性が悪用された場合、URLエンコーディングの不適切な取り扱いにより、リモートの攻撃者が予期しない状態を引き起こす可能性があります。
CVE-2024-48867, CVE-2024-48868: この脆弱性が悪用された場合、CRLFシーケンスの不適切な無効化により、リモートの攻撃者にアプリケーションデータを改ざんされる可能性があります。
CVE-2024-50393: この脆弱性が悪用された場合、コマンドインジェクションにより、リモートの攻撃者により悪意のあるコマンドを実行される可能性があります。
CVE-2024-50402, CVE-2024-50403: この脆弱性が悪用された場合、外部から制御されるフォーマット文字列により、管理者アクセスを持つリモートの攻撃者により秘密のデータを取得されたり、メモリを変更されたりする可能性があります。

ステータス：解決済み
対策手段：対象となるOSを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QTS 5.1.x | QTS 5.1.9.2954 build 20241120 以降 |
| QTS 5.2.x | QTS 5.2.2.2950 build 20241114 以降 |
| QuTS hero h5.1x | QuTS hero |

| | |
|---|---|
| | h5.1.9.2954 build 202 41120 以降 |
| QuTS hero h5.2x | QuTS hero h5.2.2.2952 build 202 41116 以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QTS and QuTS hero (PWN2OWN 2024)

---

**ライセンス センター の脆弱性**

最終更新日：2024年 12月 7日
セキュリティID：QSA-24-50
危険度：**重要**
CVE識別子:CVE-2024-48863
影響を受ける製品：ライセンス センター 1.9.x

ライセンス センターに影響を及ぼすコマンド インジェクションの脆弱性が報告されています。この脆弱性が悪用されると、リモートの攻撃者が任意のコマンドを実行できる可能性があります。

ステータス：解決済み
対策手段：対象となるLicense Centerを利用している場合には、下記の修正/対策済みバージョンへアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| ライセンス センター 1.9.x | ライセンス センター 1.9.43 以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in License Center

---

**Notes Station 3 の脆弱性**

最終更新日：2024年 11月 23日
セキュリティID：QSA-24-36
危険度：**重要**
CVE識別子:CVE-2024-38643,CVE-2024-38644,CVE-2024-38645,CVE-2024-38646
影響を受ける製品：Notes Station 3 version 3.9.x

Notes Station 3 に影響を及ぼす複数の脆弱性が報告されています。

CVE-2024-38643
重要な機能の認証が欠落している脆弱性につき、これが悪用された場合にリモートの攻撃者からシステムにアクセスされる可能性があります。
CVE-2024-38644
コマンド インジェクションの脆弱性につき、これが悪用された場合にリモートの攻撃者が任意のコマンドを実行

できる可能性があります。
CVE-2024-38645
サーバー側リクエストフォージェリ (SSRF) の脆弱性につき、これが悪用された場合にリモートの攻撃者がアプリケーションデータを読み取ることができる可能性があります。
CVE-2024-38646
重要なリソースに対する不正な権限割当ての脆弱性により、管理者アクセス権を取得したローカルの攻撃者がデータに不正にアクセスできる可能性があります。

ステータス：解決済み
対策手段：対象となるNotes Station3を利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| Notes Station 3 version 3.9.x | Notes Station 3 version 3.9.7以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in Notes Station 3

---

## QNAP AI Core の脆弱性

最終更新日：2024年 11月 23日
セキュリティID：QSA-24-40
危険度：**重要**
CVE識別子:CVE-2024-38647
影響を受ける製品：QNAP AI Core 3.4.x

QNAP AI Coreに機密情報の漏洩の脆弱性が影響していると報告されています。この脆弱性が悪用されると、リモートの攻撃者がシステムのセキュリティを侵害する可能性があります。

ステータス：解決済み
対策手段：対象となるQNAP AI Coreを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QNAP AI Core 3.4.x | QNAP AI Core 3.4.1 以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in QNAP AI Core

---

## QuLog Center に複数の脆弱性

最終更新日：2024年 11月 23日
セキュリティID：QSA-24-46
危険度：**重要**

CVE識別子:CVE-2024-48862
影響を受ける製品：QuLog Center 1.7.x 及び1.8.x

リンク追跡の脆弱性がQuLog Centerに影響を与えることが報告されています。この脆弱性が悪用されると、リモートの攻撃者がファイルシステムをトラバースして意図しない場所に移動できる可能性があります。

ステータス：解決済み
対策手段：対象となるQuLog Centerを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QuLog Center 1.7.x | QuLog Center 1.7.0.831 (2024/10/15) 以降 |
| QuLog Center 1.8.x | QuLog Center 1.8.0.888 (2024/10/15) 以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in QuLog Center

---

**QTS および QuTS hero に複数の脆弱性**

最終更新日：2024年 11月 23日
セキュリティID：QSA-24-43
危険度：**重要**
CVE識別子:CVE-2024-37041,CVE-2024-37042,CVE-2024-37043,CVE-2024-37044,CVE-2024-37045,CVE-2024-37046,CVE-2024-37047,CVE-2024-37048,CVE-2024-37049,CVE-2024-37050,CVE-2024-50396,CVE-2024-50397,CVE-2024-50398,CVE-2024-50399,CVE-2024-50400
影響を受ける製品：QTS 5.2.x、QuTS hero h5.2.x

特定の QNAPオペレーティングシステムバージョンに影響を及ぼす複数の脆弱性が報告されています。

CVE-2024-37041,CVE-2024-37044,CVE-2024-37047,CVE-2024-37049,CVE-2024-37050
この脆弱性が悪用された場合、管理者権限を持つ遠隔攻撃者によりメモリ書き換えやプロセスクラッシュの危険があります。
CVE-2024-37042,CVE-2024-37045,CVE-2024-37048:
この脆弱性が悪用された場合、管理者権限を持つ遠隔攻撃者によりサービス拒否（DoS）攻撃を起動される危険があります。
CVE-2024-37043,CVE-2024-37046
この脆弱性が悪用された場合、管理者権限を持つ遠隔攻撃者により想定されないファイルやシステムデータを読み出される危険があります。
CVE-2024-50396,CVE-2024-50397,CVE-2024-50398,CVE-2024-50399,CVE-2024-50400,CVE-2024-50401
この脆弱性が悪用された場合、遠隔攻撃者により秘密のデータを取得されたりメモリを書き換えられたりする危険があります。

ステータス：解決済み
対策手段：対象となるOSを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QTS 5.2.x | QTS 5.2.1.2930 build 20241025 以降 |
| QuTS hero h5.2x | QuTS hero h5.2.1.2929 build 20241025 以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QTS and QuTS hero

---

**QuRouter の脆弱性2**

最終更新日：2024年 11月 23日
セキュリティID：QSA-24-44
危険度：**重要**
CVE識別子:CVE-2024-48860,CVE-2024-48861
影響を受ける製品：QuRouter 2.4.x

CVE-2024-48860,CVE-2024-48861
コマンド インジェクションの脆弱性が悪用された場合に、リモートの攻撃者が任意のコマンドを実行できる可能性があります。

ステータス：解決済み
対策手段：
対象となるQuRouterを利用している場合には、下記の修正/対策
済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QuRouter 2.4.x | QuRouter 2.4.3.106 以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QuRouter

---

**QuRouter の脆弱性**

最終更新日：2024年 11月 04日
セキュリティID：QSA-24-45
危険度：**高**
CVE識別子:CVE-2024-50389
影響を受ける製品：QuRouter 2.4.x

CVE-2024-50389
QuRouterに影響を与える脆弱性が報告されています。

ステータス：解決済み
対策手段：

対象となるQuRouterを利用している場合には、下記の修正/対策
済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| QuRouter 2.4.x | QuRouter 2.4.5.032 以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in QuRouter (PWN2OWN 2024)

---

**SMB Service の脆弱性**

最終更新日：2024年 10月 30日
セキュリティID：QSA-24-42
危険度：**高**
CVE識別子:CVE-2024-50387
影響を受ける製品：SMB Service 4.15.x, SMB Service h4.15.x

CVE-2024-50387
この脆弱性が悪用された場合、リモートの攻撃者がNASシステムを悪用し、ルートシェルを取得する可能性があります。

ステータス：解決済み
対策手段：対象となるSMB Serviceを利用している場合には、下記の修正/対策済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正済みバージョン |
|---|---|
| SMB Service 4.15.x | SMB Service 4.15.002 以降 |
| SMB Service h4.15.x | SMB Service h4.15.002 以降 |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in SMB Service (PWN2OWN 2024)

---

**HBS 3 Hybrid Backup Sync の脆弱性**

最終更新日：2024年 10月 29日
セキュリティID：QSA-24-41
危険度：**高**
CVE識別子:CVE-2024-50388
影響を受ける製品：HBS 3 Hybrid Backup Sync 25.1.x

CVE-2024-50388
この脆弱性が悪用された場合、該当デバイス上でリモート攻撃者から任意のコマンドを実行される可能性があります。

ステータス：解決済み
対策手段：対象となるHBS 3 Hybrid Backup

Syncを利用している場合には、下記の修正/対策
済みバージョン、或いはそれ以降の最新版へアップデートしてください。

| アップデート対象バージョン | 修正対策済みバージョン | OS |
|---|---|---|
| Hybrid Backup Sync 25.1.x | HBS 3 Hybrid Backup Sync 25.1.1.673 以降 | QTS 5.2.x, 5.1.x QuTS hero h5.2.x, h5.1.x |

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in HBS 3 Hybrid Backup Sync (PWN2OWN 2024)

---

**QTS , QuTS heroの複数の脆弱性**

最終更新日：2024年 9月7日
セキュリティID：QSA-24-33
危険度：重要
CVE識別子:CVE-2024-21906/CVE-2024-32763/CVE-2024-38641

影響を受ける製品：QTS 5.1.x, QuTS hero h5.1.x

概要：該当OSに複数の脆弱性が報告されています。

**CVE-2024-21906**
この脆弱性が悪用された場合、入力サイズがチェックされないバッファコピーの脆弱性により、リモートの攻撃者に悪意のあるコードを実行されるおそれがあります。
**CVE-2024-32763**
この脆弱性が悪用された場合、OSコマンドインジェクションの脆弱性により、ユーザーアクセスを得たローカルの攻撃者に悪意のあるコマンドを注入されるおそれがあります。
**CVE-2024-38641**
この脆弱性が悪用された場合、OSコマンドインジェクションの脆弱性により、管理者アクセスを得たリモートの攻撃者に悪意のあるコマンドを注入されるおそれがあります。

ステータス：解決済み

対策手段：対象となるOSの各バージョンを利用している場合には、下記の修正/対策済みバージョンへアップデートしてください。

- QTS 5.1.8.2823 build 20240712 またはそれ以降
- QuTS hero h5.1.8.2823 build 20240712 またはそれ以降

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QTS and QuTS hero

---

**Video Station の脆弱性**

最終更新日：2024年 9月7日
セキュリティID：QSA-24-24
危険度：重要
CVE識別子:CVE-2023-47563/CVE-2023-50360

影響を受ける製品：Video Station 5.x

概要：Video Stationに複数の脆弱性が報告されています。

**CVE-2023-47563**
この脆弱性が悪用された場合、OSコマンドインジェクションの脆弱性により、リモートの攻撃者にアプリケーションの入力を通じて悪意のあるコマンドを実行されるおそれがあります。
**CVE-2023-50360**
この脆弱性が悪用された場合、SQLインジェクションの脆弱性により、攻撃者に悪意のあるコードを注入されるおそれがあります。

ステータス：解決済み

対策手段：対象となるVideo
Stationを利用している場合には、下記の修正/対策済みバージョンへアップデートしてください。

- Video Station 5.8.2 またはそれ以降

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerabilities in Video Station

---

**QTS、QuTS hero、および QuTScloud の脆弱性**

最終更新日：2024年4月25日
セキュリティID：QSA-24-14
危険度：**高**
CVE識別子:CVE-2023-51364/CVE-2023-51365

影響を受ける製品：QTS 5.1.x, 4.5.x ; QuTS hero h5.1.x, h4.5.x ; QuTScloud c5.x

概要：該当OSに複数の脆弱性が報告されています。

**CVE-2023-51364/CVE-2023-51365**
この脆弱性が悪用された場合、パストラバーサル
脆弱性により、
予期されないファイルが読み出され、重要なデータがネットワーク上にさらされる恐れがあります。

ステータス：解決済み

対策手段：対象となるOSの各バージョンを利用している場合には、下記の修正/対策済みバージョンへアップデートしてください。

- QTS 5.1.4.2596 build 20231128 またはそれ以降
- QTS 4.5.4.2627 build 20231225 またはそれ以降
- QuTS hero h5.1.3.2578 build 20231110 またはそれ以降
- QuTS hero h4.5.4.2626 build 20231225 またはそれ以降
- QuTScloud c5.x QuTScloud c5.1.5.2651 またはそれ以降

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QTS, QuTS hero, and QuTScloud (PWN2OWN 2023)

---

**Media Streamingの脆弱性**

最終更新日：2024年4月25日
セキュリティID：QSA-24-15

危険度：**高**
CVE識別子:CVE-2023-47222

影響を受ける製品：Media Streaming add-on 500.1.x

概要：Media Streaming add-onに、複数の脆弱性が報告されています。

この脆弱性が悪用された場合、認証されたユーザーにより
ネットワーク経由でコマンドを実行される、悪意あるコードを挿入される などのおそれがあります。

ステータス：解決済み

対策手段：対象となるMedia Streaming add-
onの各バージョンを利用している場合には、下記の対策済みバージョンへアップデートしてください。

- Media Streaming add-on 500.1.1.5 (2024/01/22) またはそれ以降

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。
尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Vulnerability in Media Streaming Add-on

---

**QTS、QuTS hero、QuTScloud、および myQNAPcloud の脆弱性**

最終更新日：2024年3月9日
セキュリティID：QSA-24-09
危険度：**緊急**
CVE識別子:CVE-2024-21899/CVE-2024-21900/CVE-2024-21901

影響を受ける製品：QTS 5.1.x、4.5.x、QuTS hero h5.1.x、h4.5.x、QuTScloud c5.x、myQNAPcloud 1.0.x

概要：該当OSに複数の脆弱性が報告されています。

**CVE-2024-21899**
この脆弱性が悪用された場合、不適切な認証の脆弱性により、ネットワーク経由で
システムのセキュリティが侵害されるおそれがあります。

**CVE-2024-21900**
この脆弱性が悪用された場合、インジェクション脆弱性
により、認証されたユーザーによりネットワーク経由でコマンドを実行されるおそれがあります。

**CVE-2024-21901**
この脆弱性が悪用された場合、SQLインジェクション脆弱性
により、認証されたユーザーによりネットワーク経由で悪意あるコードを挿入されるおそれがあります。

ステータス：解決済み

対策手段：対象となるOSの各バージョンを利用している場合には、下記の修正/対策済みバージョンへアップデートしてください。

- QTS 5.1.x: QTS 5.1.3.2578 build 20231110 またはそれ以降
- QTS 4.5.x: QTS 4.5.4.2627 build 20231225 またはそれ以降
- QuTS hero h5.1.x: QuTS hero h5.1.3.2578 build 20231110 またはそれ以降
- QuTS hero h4.5.x: QuTS hero h4.5.4.2626 build 20231225 またはそれ以降
- QuTScloud c5.x: QuTScloud c5.1.5.2651 またはそれ以降
- myQNAPcloud 1.0.x: myQNAPcloud 1.0.52 (2023/11/24) またはそれ以降

※これらの詳細手順は以下のリンク先メーカーウェブサイトページの記載情報を参照してください。

尚、こちらは英語版のみの提供につき、ご利用にあたってはWebブラウザのページ翻訳機能などをご利用ください。

詳細・対策実施手順掲載ページ：Multiple Vulnerabilities in QTS, QuTS hero, QuTScloud, and myQNAPcloud

一意的なソリューション ID: #1002
製作者:
最終更新: 2026-04-14 16:54