QNAP

QNAP-NAS 脆弱性関連情報ポータル 2024

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 ※2024年 12月9日 更新

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。

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	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)

QNAP

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

---

QNAPのQuMagieの脆弱性

最終更新日：2023年11月11日
セキュリティID：QSA-23-50
危険度：**高**
CVE識別子:CVE-2023-39295 / 2023-41284 / 2023-41285

影響を受ける製品：QuMagie 2.1.x

概要：QuMagieに影響を与える複数の脆弱性が報告されています。

CVE-2023-39295:
OSコマンドインジェクションの脆弱性が悪用された場合、認証されたユーザーからネットワーク経由でコマンドを実行される可能性があります。

CVE-2023-41284/41285
SQLインジェクションの脆弱性が悪用された場合、認証されたユーザーからネットワーク経由で悪意のあるコードを挿入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。

- QuMagie 2.1.4 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 QuMag

QTS および QuTS hero の脆弱性

最終更新日：2023年11月4日
セキュリティID：QSA-23-31
危険度：**緊急**

影響を受ける製品：QTS 5.0.x, 4.5.x; QuTS hero h5.0.x, h4.5.x; QuTScloud c5.0.1

概要：該当OS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。
この脆弱性が悪用された場合、リモートを介した攻撃者から任意のコマンドを実行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、下記の対策済みバージョンへアップデートしてください。

- QTS 5.0.1.2376 build 20230421 またはそれ以降
- QTS 4.5.4.2374 build 20230416 またはそれ以降

- QuTS hero h5.0.1.2376 build 20230421 またはそれ以降
- QuTS hero h4.5.4.2374 build 20230417 またはそれ以降
- QuTScloud c5.0.1.2374 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 QTS, QuTS hero, and QuTScloud

---

QTS, Multimedia Console, 及びMedia Streaming add-on の脆弱性

最終更新日：2023年11月4日
セキュリティID：QSA-23-35
危険度：**緊急**

影響を受ける製品：QTS 5.1.x, 4.3.6, 4.3.4, 4.3.3, 4.2.x; Multimedia Console 2.1.x, 1.4.x; Media Streaming add-on 500.1.x, 500.0.x

概要：該当OS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。
この脆弱性が悪用された場合、リモートを介した第三者から任意のコマンドを実行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 5.1.0.2399 build 20230515 またはそれ以降
- QTS 4.3.6.2441 build 20230621 またはそれ以降
- QTS 4.3.4.2451 build 20230621 またはそれ以降
- QTS 4.3.3.2420 build 20230621 またはそれ以降
- QTS 4.2.6 build 20230621 またはそれ以降

- Multimedia Console 2.1.2 (2023/05/04) またはそれ以降
- Multimedia Console 1.4.8 (2023/05/05) またはそれ以降
- Media Streaming add-on 500.1.1.2 (2023/06/12) またはそれ以降
- Media Streaming add-on 500.0.0.11 (2023/06/16) 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 QTS, Multimedia Console, and Media Streaming add-on

---

QUSBCam2 の脆弱性

最終更新日：2023年10月21日
セキュリティID：QSA-23-43
危険度：高
影響を受ける製品：QUSBCam2 2.0.x

概要：QNAPのQUSBCam2 2.0.x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。
この脆弱性が悪用された場合、ネットワークを介して第三者から任意のコマンドを実行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QUSBCam2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。

- QUSBCam2 2.0.3 (2023/06/15) 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 QUSBCam2

QTS および QuTS hero の脆弱性

最終更新日：2023年10月14日
セキュリティID：QSA-23-42
危険度：高
影響を受ける製品：QTS 5.1.x, QuTS hero h5.1.x, QuTScloud c5.x

概要：該当OSに、パストラバーサル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、第三者に重要な情報を読み出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 5.1.0.2444 build 20230629 またはそれ以降
- QuTS hero h5.1.0.2424 build 20230609 またはそれ以降
- QuTScloud c5.1.0.2498 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 QTS, QuTS hero, and QuTScloud

---

Video Station の脆弱性

最終更新日：2023年10月14日
セキュリティID：QSA-23-52
危険度：高
影響を受ける製品：Video Station 5.7.x

概要：QNAPのVideo Stationに、3件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悪意の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Video Station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。

- Video Station 5.7.0 (2023/07/27) 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

Music Station の脆弱性

最終更新日：2023年10月7日
セキュリティID：QSA-23-28
危険度：**高**
影響を受ける製品：Music Station 5.3.x

概要：QNAPの Music Station に、ツーパストラバーサル脆弱性(Two path traversal vulnerabilities)が報告されています。この脆弱性が悪用された場合、第三者にネットワーク越しに情報を参照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Music Station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。

- Music Station 5.3.22 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 Music Station

Multimedia Console の脆弱性

最終更新日：2023年9月22日
セキュリティID：QSA-23-29
危険度：**高**
影響を受ける製品：Multimedia Console 2.1, 1.4

概要：QNAPの複数の Multimedia Console に、バッファの入力サイズをチェックしない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、想定外のコードを実行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Multimedia Console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。

- Multimedia Console 2.1.1 (2023/03/29) またはそれ以降
- Multimedia Console 1.4.7 (2023/03/20) 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 Multimedia Console

QTSの旧バージョンの脆弱性

最終更新日：2023年9月22日
セキュリティID：QSA-23-25
危険度：**高**
影響を受ける製品：QTS 4.3.6, 4.3.4, 4.3.3, 4.2.6

概要：該当OSに、バッファの入力サイズをチェックしない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、想定外のコードを実行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、下記の対策済みバージョンへアップデートしてください。

- QTS 4.3.6.2441 build 20230621 またはそれ以降
- QTS 4.3.4.2451 build 20230621 またはそれ以降
- QTS 4.3.3.2420 build 20230621 またはそれ以降
- QTS 4.2.6 build 20230621 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 Legacy QTS

QTS および QuTS hero の脆弱性

最終更新日：2023年9月16日
セキュリティID：QSA-23-18
危険度：**高**
影響を受ける製品：QTS 5.0.1, 4.5.4; QuTS hero h5.0.1, h4.5.4; QuTScloud c5.0.1

概要：該当OS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。
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コマンドを実行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、下記の対策済みバージョンへアップデートしてください。

- QTS 5.0.1.2376 build 20230421またはそれ以降
- QTS 4.5.4.2374 build 20230416 またはそれ以降
- QuTS hero h5.0.1.2376 build 20230421 またはそれ以降
- QuTS hero h4.5.4.2374 build 20230417 またはそれ以降
- QuTScloud c5.0.1.2374 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 QTS, QuTS hero, and QuTScloud

---

QTS および QuTS hero の脆弱性

最終更新日：2023年9月8日
セキュリティID：QSA-23-13
危険度：**高**
影響を受ける製品：QuLog Center 1.5, 1.4, 1.3

概要：QNAPの複数のOSのQuLOG Centerに、クロスサイトスクリプティング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、悪意の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QTS、及びQuTS heroの各バージョンを利用している場合には、QuLOG Centerを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。

- QTS 5.0.1: QuLog Center 1.5.0.738 (2023/03/06) またはそれ以降
- QTS 4.5.4: QuLog Center 1.3.1.645 (2023/02/22) またはそれ以降

- QuTS hero h5.0.1: QuLog Center 1.5.0.738 (2023/03/06) またはそれ以降
- QuTS hero h4.5.4: QuLog Center 1.3.1.645 (2023/02/22) またはそれ以降
- QuTscloud c5.0.1: QuLog Center 1.4.1.691 (2023/03/01) 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 QuLog Center on QTS, QuTS hero and QuTScloud

---

QTS および QuTS hero の脆弱性

最終更新日：2023年8月25日
セキュリティID：QSA-23-60
危険度：**高**
影響を受ける製品：QTS 5.1.0, 5.0.1, 4.5.4; QuTS hero h5.1.0, h4.5.4

概要：不適切な強度の暗号化について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、ローカルネットワーククライアントによりブルートフォース攻撃で複合化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QTS、及びQuTS hero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。

- QTS 5.1.0.2444 ビルド 20230629 またはそれ以降
- QTS 5.0.1.2425 ビルド 20230609 またはそれ以降
- QTS 4.5.4.2467 ビルド 20230718 またはそれ以降
- QuTS hero h5.1.0.2424 ビルド 20230609 またはそれ以降
- QuTS hero h4.5.4.2476 ビルド 20230728 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 QTS and QuTS hero

QTS および QuTS hero の脆弱性

最終更新日：2023年7月28日
セキュリティID：QSA-23-09
危険度：**高**
影響を受ける製品：一部のQNAP製機器

概要：QNAP社製NAS上で実行される複数の専用OSに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、リモートからの攻撃者によってDoS攻撃が実行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QTS、及びQuTS hero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。

- QTS 5.0.1.2277 ビルド 20230112 以降
- QTS 4.5.4.2280 ビルド 20230112 以降
- QuTS hero h5.0.1.2277 ビルド 20230112 以降
- QuTS hero h4.5.4.2374 ビルド 20230417 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 QTS and QuTS hero

QTS および QuTS hero の脆弱性（sudoコマンド関連）

最終更新日：2023年6月16日
セキュリティID：QSA-23-11
危険度：**高**
CVE識別子：CVE-2023-22809
影響を受ける製品：一部のQNAP NAS製品

概要：QNAP社製NASの以下のOSの sudo コマンドに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、リモートからの攻撃者によって悪意のあるコードが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QTS、及びQuTS hero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。

- QTS 5.0.1.2346 ビルド 20230322 以降
- QuTS hero h5.0.1.2348 ビルド 20230324 以降

※5/30付 追加対応分

- QTS 4.5.4.2374 build 20230416 and later
- QuTS hero h4.5.4.2374 build 20230417 and later
- QuTScloud c5.0.1.2374 and later
- QVP 2.3.1.0476 and later

※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 sudo

QTS および QuTS hero の脆弱性

最終更新日：2023年1月30日
セキュリティID：QSA-23-01
危険度：**重大**
影響を受ける製品：QTS5.0.1 および QuTS hero h5.0.1 を実行しているQNAP-NAS

概要：QNAP社製NAS上で実行される複数の専用OSに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、リモートからの攻撃者によって悪意のあるコードが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QTS、及びQuTS hero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。

QTS 5.0.1.2234 ビルド 20221201 以降
QuTS hero h5.0.1.2248 ビルド 20221215 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 QTS and QuTS hero

一意的なソリューション ID: #1002
製作者:
最終更新: 2024-12-10 15:47