

セキュリティ調査レポート

対象ホスト 192.0.2.10

この PDF は保存済みのタスク・資産・検出を1台分にまとめたものです。作成時に新しい調査は行っていません。

公開サンプルです。実在の調査結果をもとにしていますが、ホストや製品を特定できる記載は一般化しています。検出の件数、種類、重大度、状態、影響と対処の方向は元の結果に沿っています。

- IPアドレスは文書用の予約アドレス 192.0.2.10（RFC 5737）です。
- タスクIDは連番に振り直しています。
- 製品名、版番号、実装固有の名称、個体の特定につながる非標準ポートは、役割が分かる表現に置き換えています。置き換えたポートは「—」です。

関連タスク（3）

ID	名称	状態	目標
#1	192.0.2.10	完了	脆弱性の発見
#2	192.0.2.10	実行中	脆弱性の発見
#3	192.0.2.10	実行中	脆弱性の発見

観測した資産（13）

種別	宛先	ポート	サービス
ip	192.0.2.10	—	—
service	192.0.2.10	139	smb
service	192.0.2.10	443	https
service	192.0.2.10	445	smb
service	192.0.2.10	548	afp
service	192.0.2.10	3702	ws-discovery
service	192.0.2.10	—	nas-internal-api
service	192.0.2.10	—	http-app
service	192.0.2.10	5355	llmnr
service	192.0.2.10	—	nas-admin-ui
service	192.0.2.10	—	git-hosting
service	192.0.2.10	—	http-nginx
endpoint	https://192.0.2.10/admin/	—	NAS管理UI（ログイン画面）

検出事項（8）

NAS内部APIのログイン判定不備。未認証で通知ログ・設定値・管理者ユーザ名が取得できる

重大度: 中 / 状態: 未確認 / タスク #3

影響 認証を経ずに、内部の設定・ログ・利用者が読める。ログイン済みかどうかの判定が、接続先の名前に依存している。

対処 このAPIを認証必須にする。接続先の名前だけでログイン済みと判断しない。到達範囲を管理用ネットワークに限る。

NAS内部APIの未認証エンドポイント露出と、通知ログ・管理者ユーザ名・設定値の情報漏えい

重大度: 中 / 状態: 未確認 / タスク #3

影響 認証前に内部情報へ到達できる。

対処 認証を必須にし、管理用ネットワーク以外からは到達できないようにする。

NAS管理UIのTLS証明書が期限切れ

重大度: 中 / 状態: 未確認 / タスク #3

影響 管理通信で証明書の失効を検知しにくく、警告を無視する運用になりやすい。

対処 証明書を更新し、期限の監視を入れる。

ソース管理（Gitホスティング）の公開と、版に依存した既知の欠陥の可能性

重大度: 中 / 状態: 未確認 / タスク #3

影響 ソース管理へネットワークから到達でき、版に依存した既知の欠陥が残る可能性がある。

対処 認証とネットワーク制限を確認し、保守されている版へ更新する。

NAS内部APIの未認証露出

重大度: 中 / 状態: 未確認 / タスク #3

影響 認証前に内部情報へ到達できる。

対処 認証を必須にし、管理用ネットワーク以外からは到達できないようにする。

ファイル共有（SMB / AFP）の未認証露出と、内部名・ワークグループ情報の開示

重大度: 中 / 状態: 未確認 / タスク #3

影響 ファイル共有と内部の名前が、ネットワーク上から分かる。

対処 匿名アクセスを止め、必要な端末だけに制限する。

Webサーバ（nginx）のバージョン情報開示。公開されている版は既知の欠陥の対象になり得る

重大度: 中 / 状態: 未確認 / タスク #3

影響 製品の系統が外部から判別でき、既知の欠陥の対象になり得る。

対処 サポートされる版へ更新し、不要なバージョン表示を隠す。

NAS管理UIのログイン画面と静的ファイルが認証不要で公開（CSP に unsafe-inline / unsafe-eval、HSTS無し）

重大度: 低 / 状態: 未確認 / タスク #3

影響 管理画面の入口が認証前に見え、ブラウザ側の防御ヘッダが弱い。

対処 管理画面を認証とネットワークの両方で制限する。CSPを厳しくし、HSTSを有効にする。