Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 29 年 10 月 17 日

Topic

ReadyNAS Surveillance の脆弱性を標的としたアクセスの観測について

ReadyNAS Surveillance の脆弱性を標的とするアクセスを観測しました。脆弱性の影響を受けるサーバに対する攻撃活動が実施されている可能性があるため、サーバの管理者等は影響有無の確認及び適切な対策を早急に実施することを推奨します。

1 ReadyNAS Surveillance の脆弱性を標的としたアクセスの観測について

ReadyNAS Surveillance は、NETGEAR 社製ファイルサーバ ReadyNAS 上で動作するネットワークビデオレコーダソフトウェアです。同ソフトウェアについて、平成 29 年9月 28 日に NETGEAR 社から脆弱性が公表[i]されました。また、その前日には、海外のセキュリティブログにおいて PoC[ii] が公表されていることを確認しています。当該脆弱性が悪用された場合、認証なしで遠隔からコマンドを実行することが可能であるとされています。

10 月9日 17 時以降、警察庁のインターネット定点観測システムにおいて、当該脆弱性を標的としていると考えられるアクセスを観測しました(図1)。

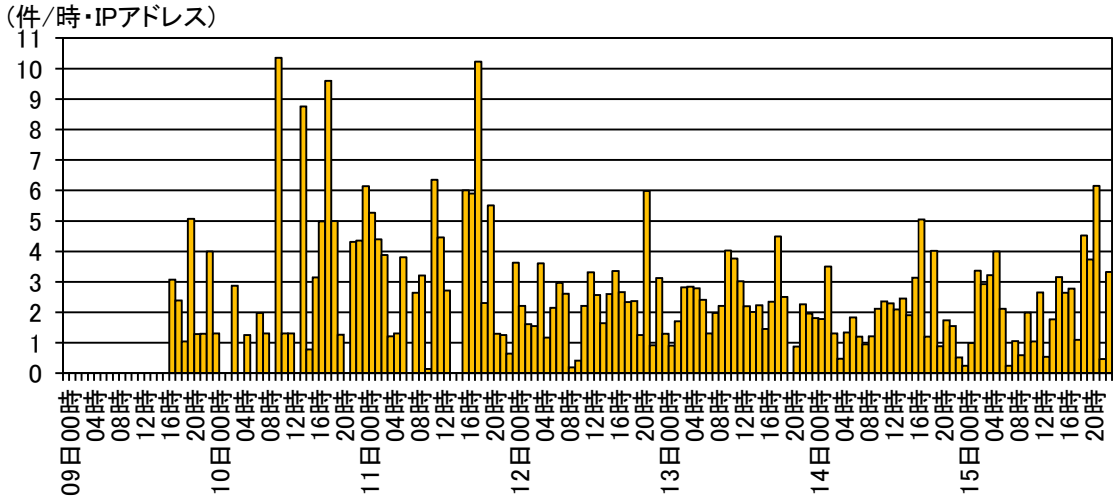

図1 ReadyNAS Surveillance の脆弱性を標的としたアクセス件数の推移
(10 月9日～10 月 15 日)

観測したアクセスは、PoC に酷似した HTTP リクエストを送信するものでした。また、そのリクエスト内容は、当該脆弱性を悪用して「/etc/passwd」ファイルの内容を表示しようとするものであり、当該脆弱性が悪用可能であるかを探索する目的だけではなく、システムに侵入す

[i] https://kb.netgear.com/000049072/Security-Advisory-for-Command-Injection-in-ReadyNAS-Surveillance-Application-PSV-2017-2653

[ii] Proof of Concept の略。脆弱性を利用した攻撃が可能であることを示すための検証用プログラム。

るための情報を収集する意図があるものと考えられます（図2）。

図2　観測したアクセスのリクエスト内容（一部マスキングを実施）

2　推奨する対策

サーバの管理者は、以下の対策を参考に、総合的にセキュリティ対策を行うことを推奨します。

- NETGEAR 社によると、当該脆弱性の影響を受けるバージョンは以下のとおりです。
  - ReadyNAS Surveillance 1.4.3-17(x86)より前
  - ReadyNAS Surveillance 1.1.4-7(ARM)より前

  これらのバージョンのソフトウェアを利用している場合は、当該脆弱性を修正したバージョンへのアップデート[i]を実施してください。
- サーバをインターネットに接続する場合には、直接インターネットに接続するのではなく、ルータ等を使用してください。また、ファイアウォール等によって不必要な外部からのアクセスを遮断する、特定の IP アドレスのみにアクセスを許可する等の適切なアクセス制限を実施してください。
- ユーザ名及びパスワードは、初期設定のままでは使用せず、必ず変更してください。また、変更する際は、ユーザ名及びパスワードを推測されにくいものにしてください。なお、使用していないユーザについては削除または無効化してください。
- 製造終了から年月が経過した製品は、製造元が脆弱性への対応を実施しない場合があります。脆弱性が存在するにも関わらず、製造元が対応しない製品は、使用を中止してください。

また、既に当該脆弱性を悪用した攻撃を受けている可能性も考えられるため、脆弱性が存在するバージョンの ReadyNAS Surveillance を利用していた場合には、サーバの動作状況や、サーバ内の不審ファイルの有無等についても、併せて確認することを推奨します。

[i] https://www.netgear.jp/supportInfo/NewSupportList/208.html