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

平成 26 年 3 月 5 日

Topic

脆弱性が存在する NAS の探索と考えられる宛先ポート 5000/TCP に対するアクセスの急増について

Synology 社製 NAS には、HTTP リクエストの処理に問題があり、攻撃者に任意のプログラムをアップロード及び実行される脆弱性[1]が明らかとなっています。同製品を使用している組織及び家庭においては、アップデートの実施等の適切な対策を早急に実施することを推奨します。

1 宛先ポート 5000/TCP に対するアクセスの急増について

警察庁の定点観測システムでは、2月 28 日以降、宛先ポート 5000/TCP に対するアクセスの急増を観測しています（図1）。

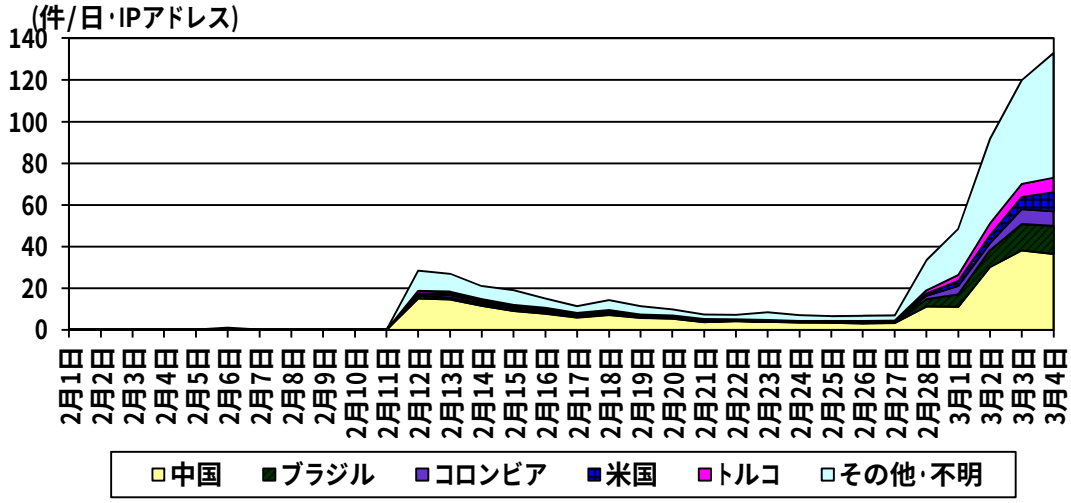

図1 宛先ポート 5000/TCP に対する発信元国・地域別アクセス件数の推移
（H26.2.1～H26.3.4）

同アクセスを分析した結果、多くのアクセスは HTTP であり、パス「/webman/info.cgi?host=」に対する GET リクエストであることが判明しました。5000/TCP は、Synology 社製 NAS のウェブ管理画面に使用されているポートです。また、同パスにアクセスして、バージョン判定を実施したうえで、その結果に基づき脆弱性を狙った攻撃を実行する攻撃コードが公開されていることも確認しています。このことから、これらのアクセスは脆弱性を持つ同製品を狙った攻撃活動であると考えられます。

[1] 「JVNVU#95919136 Synology DiskStation Manager にアクセス制御不備の脆弱性」（平成 26 年1月8日）
https://jvn.jp/vu/JVNVU95919136/index.html

2 推奨する対策

Synology 社製 NAS には、拡張モジュールにより追加可能な VPN 機能においても脆弱性[1]が明らかとなっています。同製品を使用している組織や家庭においては、以下の対策を早急に実施することを推奨します。

(1) 該当製品の確認

ア 各組織や家庭において、該当製品の使用有無を確認する。

イ 該当製品を使用している場合には、同製品の OS（DiskStation Manager）のバージョンを確認する。

ウ VPN Server モジュールのインストール有無と、インストールしていた場合には、更に同モジュールのバージョンも確認する。

(2) インターネットへの不要な公開の停止

ア インターネット上から、同製品にアクセスする必要がない場合には、インターネットへの公開を停止する。

イ インターネット上から、同製品にアクセスする必要がある場合には、ファイアーウォール等でウェブ管理画面や VPN への適切なアクセス制限を実施する。

(3) アップデートの実施

ア 同製品の OS を最新バージョンへアップデートする。

イ 同製品で使用している各種拡張モジュールについても、最新バージョンへアップデートする。

[1] 「JVNVU#97152032 Synology DiskStation Manager に認証情報がハードコードされている問題」（平成 26 年 2 月 28 日）
https://jvn.jp/vu/JVNVU97152032/index.html