平成 26 年 10 月 30 日

Topic

外部から NAT-PMP の操作が可能である機器の探索行為について

外部から NAT-PMP の操作が可能である不適切な実装の機器が多数存在する問題が報告されています。警察庁においても同機器の探索行為を観測しているため、管理する機器の設定を確認することを推奨します。

1 外部から NAT-PMP の操作が可能である機器が多数存在する問題について

NAT-PMP (NAT Port Mapping Protocol) は、ルータ等のネットワーク機器において、LAN 側に接続された機器からのリクエストに基づきアドレス及びポートのマッピングを自動的に行うためのプロトコルです。この NAT-PMP について、平成 26 年 10 月 21 日に米国のセキュリティ対策企業から、本来は受け付けてはならない WAN 側からのリクエストを受け付けてしまう機器が多数存在しているとの報告が行われました。24 日には、JPCERT/CC からも日本語による注意喚起[i]が実施されています。

NAT-PMP は、その仕様で WAN 側から受信したリクエストを受け付けてはならない等の制約が定められています。しかしながら、この制約を無視した不適切な実装がされている機器は、WAN 側からリクエストにより悪意ある操作が行われる可能性があります。NAT-PMP の外部からの操作により、次の様な攻撃が行われる可能性が指摘されています。

- トラフィックの誘導・傍受
- LAN 側機器への不正なアクセス
- NAT-PMP によるポートマッピングの運用妨害
- WAN 側アドレスやマッピング済みポートの調査

[i] 「JVNVU#99291862 複数の NAT-PMP デバイスが WAN 側から操作可能な問題」
https://jvn.jp/vu/JVNVU99291862/

2 警察庁での探索行為の観測状況

警察庁の定点観測システムでは、29 日午前3時以降 NAT-PMP で使用されるポート 5351/UDP に対する不審なアクセスを観測しています。これらのアクセスは、NAT-PMP において WAN 側の IP アドレスを問い合わせる「External Address Request」の通信でした。このことから、外部から NAT-PMP による操作が可能な機器の探索が実施されているものと考えられます。

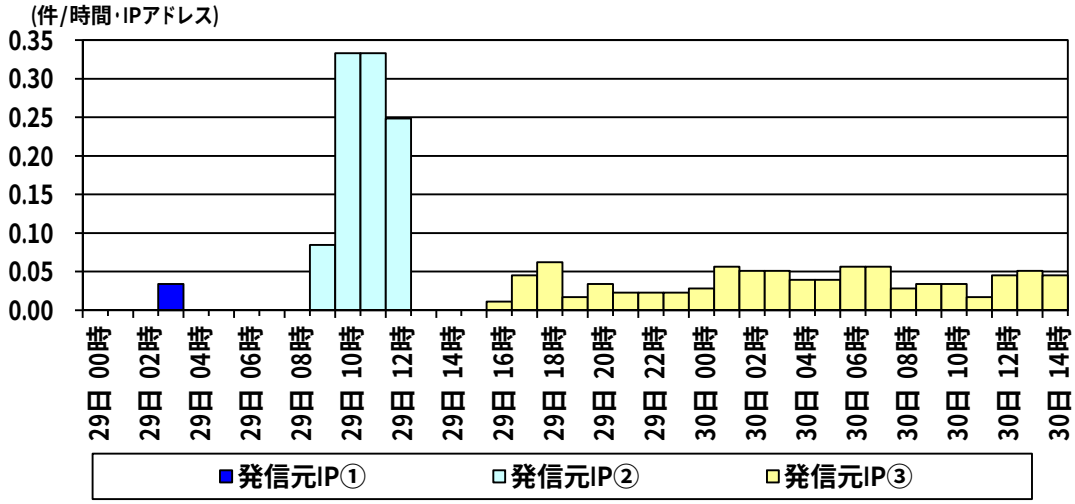

図1 宛先ポート 5351/UDP に対するアクセス件数の推移 (H26.10.29 00:00～10.30 15:00)

29 日以降、警察庁で観測している発信元 IP アドレスは大きく3種類に分類できます。

図1における発信元 IP②は、当該問題を報告した米国のセキュリティ対策企業が管理する複数の IP アドレス群であり、同企業は影響を受ける機器の台数や状況について調査を実施している旨を公表しています。このため、これらのアクセスは同調査に起因するアクセスであると考えられます。同企業からのアクセスは本年6月以降、継続して観測しています。

他方で、図1における発信元①と③は、それぞれ単一の IP アドレスですが、アクセスを行っている者の実体は判明していません。NAT-PMP による悪意ある操作を行う目的で、探索行為を実施している可能性も十分に考えられます。

3 推奨する対策

インターネットに接続しているルータ等のネットワーク機器において、以下の対策を実施することを推奨します。

(1) WAN 側からの 5351/UDP 宛の通信を制限する。
(2) NAT-PMP を無効にする。
ただし、NAT-PMP を使用している LAN 側の機器の運用に支障がでる可能性があるので、影響については十分確認を実施する。
(3) 製造メーカからのアップデートや推奨される設定変更等の情報の有無を確認し、公開されている情報がある場合には必要なアップデート等を実施する。