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

平成 28 年8月 30 日

インターネット観測結果等

（平成 28 年7月期）

- Drupal のモジュールの脆弱性を標的としたアクセスの観測
- Netis 社製ルータに対する攻撃を企図したアクセスが急増

1 Drupal のモジュールの脆弱性を標的としたアクセスの観測

平成 28 年7月 13 日に、オープンソースの CMS（コンテンツ管理システム）である Drupal のモジュール「RESTWS」に存在する深刻な脆弱性[i]が公表されました。当該脆弱性を悪用すると、特別に細工したリクエストを送信することによって、任意の PHP のコードを実行させることが可能であるとされています。また、7 月下旬には、当該脆弱性に対する探索等が可能なツールが、インターネット上で公開されていることも確認しています。

警察庁のインターネット定点観測システムにおいては、7月 21 日に当該脆弱性を標的としたアクセスを観測しました（図 1）。

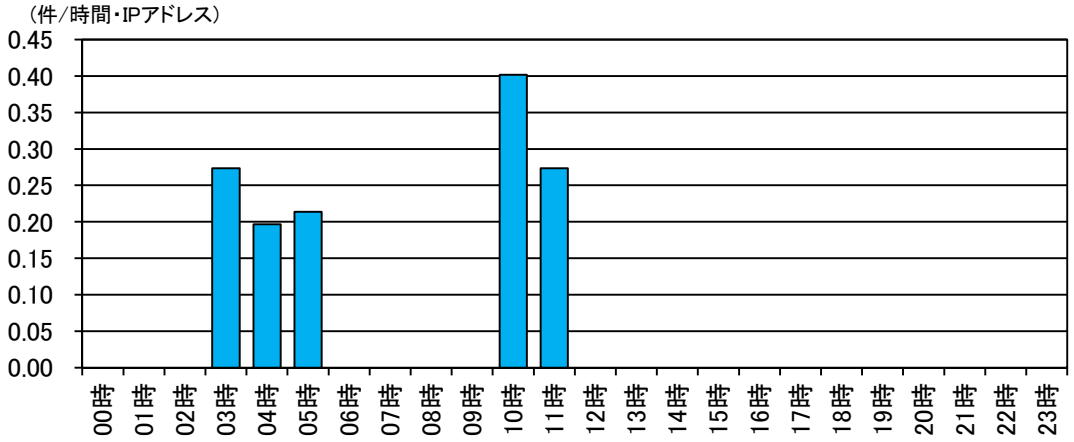

図 1 Drupal のモジュール「RESTWS」の脆弱性を標的としたアクセス（7月 21 日）

観測したアクセスは、HTTP リクエストにおいて特定の文字列を表示させるコマンドや PHP のコードを含むものでした。そのため、これらのアクセスは実際に攻撃を試みるものではなく当該脆弱性の有無を確認する探索行為であると推測されます。

当該脆弱性を悪用されると深刻な被害を受ける危険性もあるため、影響を受けるバージョンの Drupal と RESTWS を利用しているサーバの管理者は、脆弱性が修正されたバージョンへの速やかなアップデートを推奨します。

[i] RESTWS - Highly critical - Remote code execution - SA-CONTRIB-2016-040
https://www.drupal.org/node/2765567

なお、影響を受ける Drupal と RESTWS のバージョンの組合せは以下のとおりです。

- Drupal の 7.x と、RESTWS の 7.x-2.6 より前の 7.x-2.x
- Drupal の 7.x と、RESTWS の 7.x-1.7 より前の 7.x-1.x

2 Netis 社製ルータに対する攻撃を企図したアクセスが急増

Netis[i]社製のルータでは 53413/UDP のポートが使用されます。平成 26 年8月には外部から容易にアクセスできる脆弱性をセキュリティ対策企業が公表[ii]しました。警察庁のインターネット定点観測システムでは、同年8月 27 日に宛先ポート 53413/UDP に対するアクセスの急増を観測[iii]して以降、継続的に同アクセスの増加を観測[iv]しています。

今期は、7月 23 日から宛先ポート 53413/UDP に対するアクセスが急増しました（図 2）。

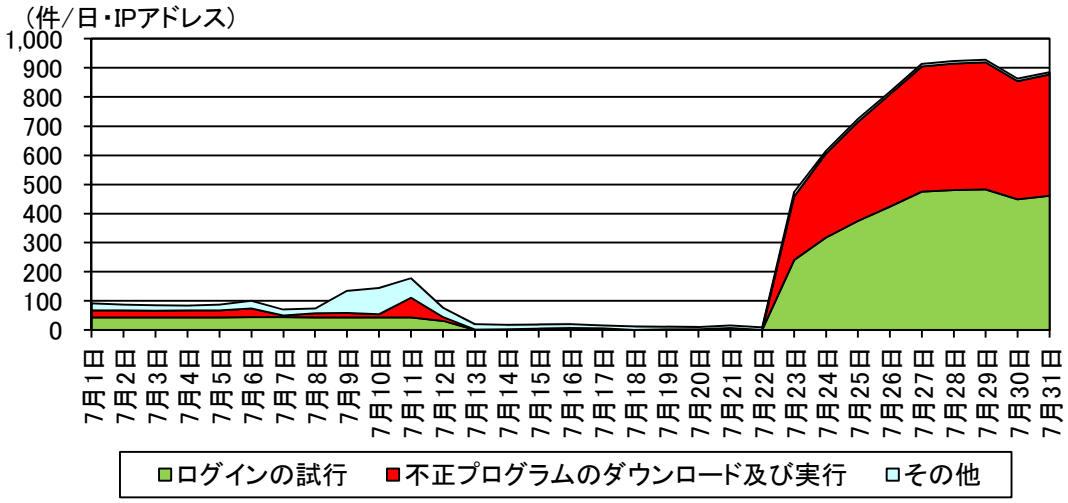

図2 宛先ポート 53413/UDP に対するアクセス件数の推移（目的別）

これらのアクセスの内容を確認したところ、ほとんどのアクセスが、当該ルータへのログインを試

---

[i] 2000 年に設立されたネットワーク機器メーカで、中国深圳市に本社を置く Netcore 社のグループ企業のひとつ。
http://www.netis-systems.com/

[ii] 「UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認」（平成 26 年8月 27 日）
http://blog.trendmicro.co.jp/archives/9725

[iii] 「インターネット観測結果等（平成 26 年8月期）」（平成 26 年 10 月7日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141007_2.pdf

[iv] 「インターネット観測結果等（平成 27年8月期）」（平成 27 年9月 25 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=16942
「インターネット観測結果等（平成 27年 12 月期）」（平成 28 年1月 25 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=17624
「IoT 機器を標的とした攻撃について」（平成 27 年 12 月 15 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=17323
「インターネット観測結果等（平成 28 年6月期）」（平成 28 年7月 29 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=18807

みた後に、不正プログラムのダウンロード及び実行を試みるものでした。また、観測したアクセスの発信元を確認したところ、日本国内からのアクセスも多く存在しました（図3）。

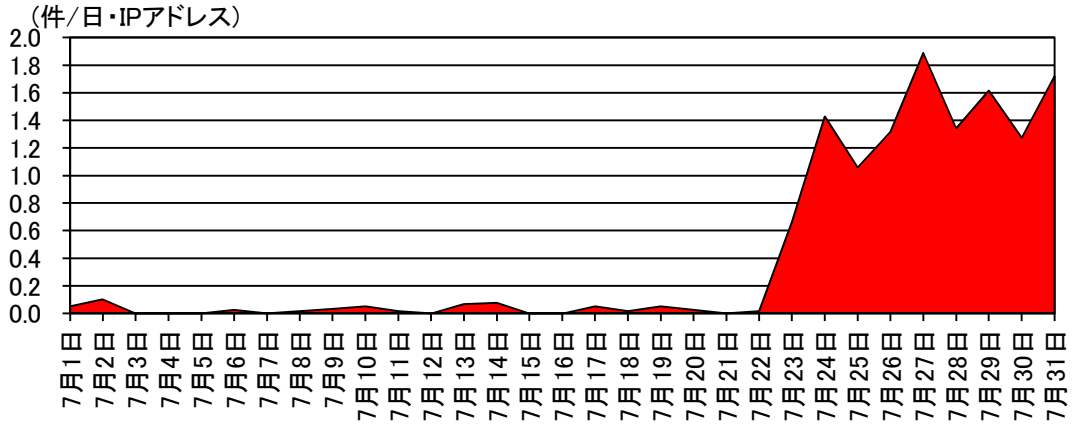

図3　宛先ポート 53413/UDP に対するアクセス件数の推移（国内）

日本国内からのアクセスの発信元を調査したところ、DVR（デジタルビデオレコーダー）、ネットワークストレージ、EMS[i]等のログイン画面が表示されるものを多数確認しました。

このことから、日本国内においても、DVR 等のインターネットに接続された機器が探索活動等の踏み台になっていると推測されます。当該ルータの脆弱性を放置したままの状態であれば、これらの発信元の機器と同様に攻撃に悪用されるおそれがあるため、適切なセキュリティ対策を実施することが必要です。

[i] EMS は、Energy Management System の略で、電気使用量の可視化や機器の制御等を行うシステムのこと。家庭向けの HEMS（Home EMS）、商用ビル向けの BEMS（Building EMS）、工場向けの FEMS（Factory EMS）及びこれらを含む地域全体向けの CEMS（Cluster/Community EMS）がある。