令和２年４月 28 日

レポート

複数の IoT 機器等の脆弱性を悪用したアクセスの観測等について

- 複数の IoT 機器等の脆弱性を悪用したアクセスの観測
- Microsoft SMBv3 の脆弱性（CVE-2020-0796）に関するアクセスの観測

１ 複数の IoT 機器等の脆弱性を悪用としたアクセスの観測

警察庁のインターネット定点観測において、複数の IoT 機器等の脆弱性を標的とするアクセスを観測しました。当該アクセスは、IoT 機器等の脆弱性を悪用し、外部サーバから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。

(1) 米国製の IP 電話交換機に SQL インジェクションの脆弱性[i]があり、令和2年3月 23 日に、PoC[ii]が公開されていることを確認しています。本脆弱性を悪用したアクセスについて3月 30 日より増加を観測しています（図1、図2）。この観測でダウンロードされるプログラムは IoT 機器に感染するバックドアと考えられるものでした。

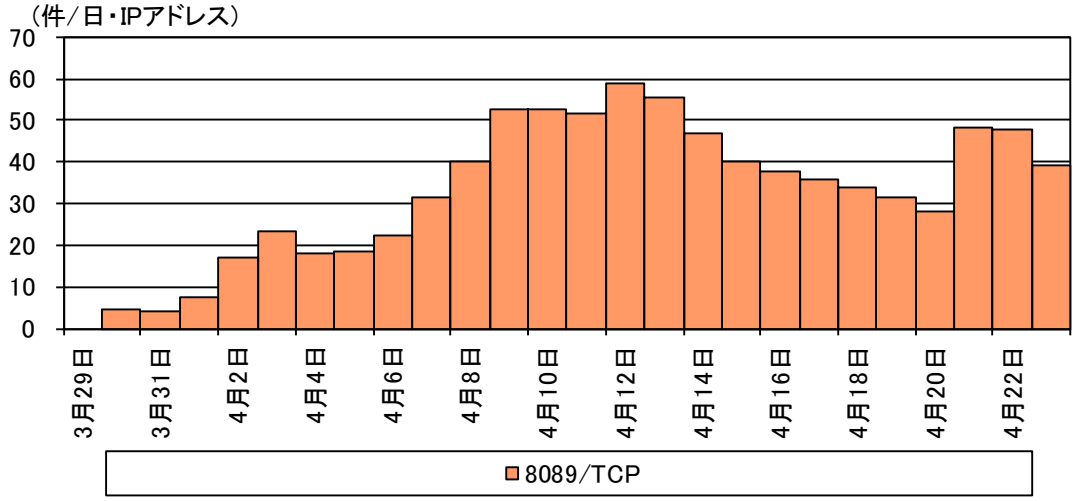

図１ 米国製 IP 電話交換機の脆弱性を悪用したアクセス件数の推移（R2.3.29～R2.4.23）

図２ 米国製 IP 電話交換機の脆弱性を悪用したアクセスの例（一部マスキングを実施）

[i] JVNDB-2020-003190(CVE-2020-5722):
https://jvndb.jvn.jp/ja/contents/2020/JVNDB-2020-003190.html

[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。

本脆弱性を悪用するアクセスの送信元 IP アドレスを調査したところ、ルータ等の機器のログイン画面が表示されることを確認しました(図3)。

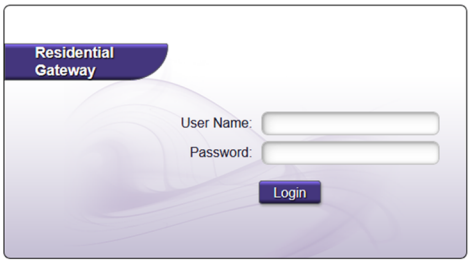

図3　送信元となっている機器のログイン画面の例

(2) 台湾製のルータにコマンドインジェクションの脆弱性[i]があり、3月 30 日に PoC が公開されていることを確認しています。本脆弱性を悪用したアクセスについて3月31日より観測しています(図4、図5)。この観測でダウンロードされるプログラムは IoT 機器に感染するバックドアと考えられるものでした。

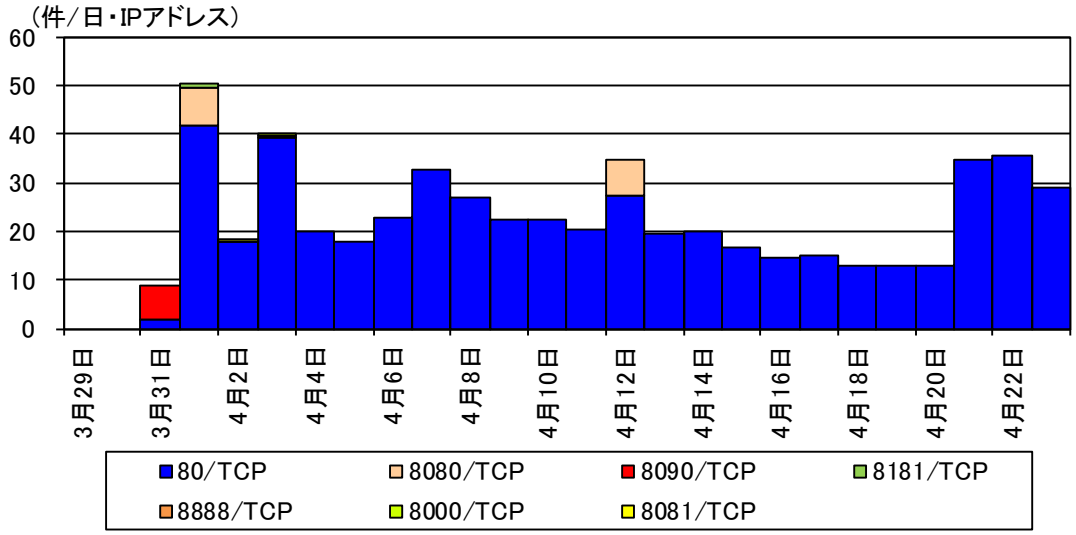

図4　台湾製ルータの脆弱性を悪用したアクセス件数の推移(R2.3.29～R2.4.23)

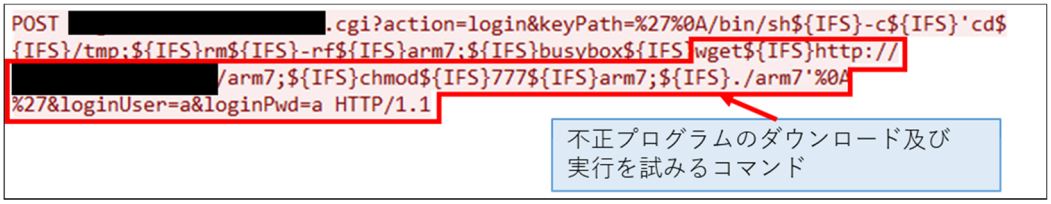

図5　台湾製ルータの脆弱性を悪用したアクセスの例(一部マスキングを実施)

[i] JVNDB-2020-001735(CVE-2020-8515):
https://jvndb.jvn.jp/ja/contents/2020/JVNDB-2020-001735.html

本脆弱性を悪用するアクセスの送信元 IP アドレスを調査したところ、IP 電話交換機等の機器のログイン画面が表示されることを確認しました（図6）。

図6　送信元となっている機器のログイン画面の例（一部マスキングを実施）

(3) インド製の GPON ルータにリモートコード実行の脆弱性があり、3月 17 日に PoC が公開されていることを確認しています。本脆弱性を悪用したアクセスについて3月　27　日より増加を観測しています（図7、図8）。この観測でダウンロードされるプログラムは IoT 機器に感染する「Mirai」の亜種と考えられるものでした。

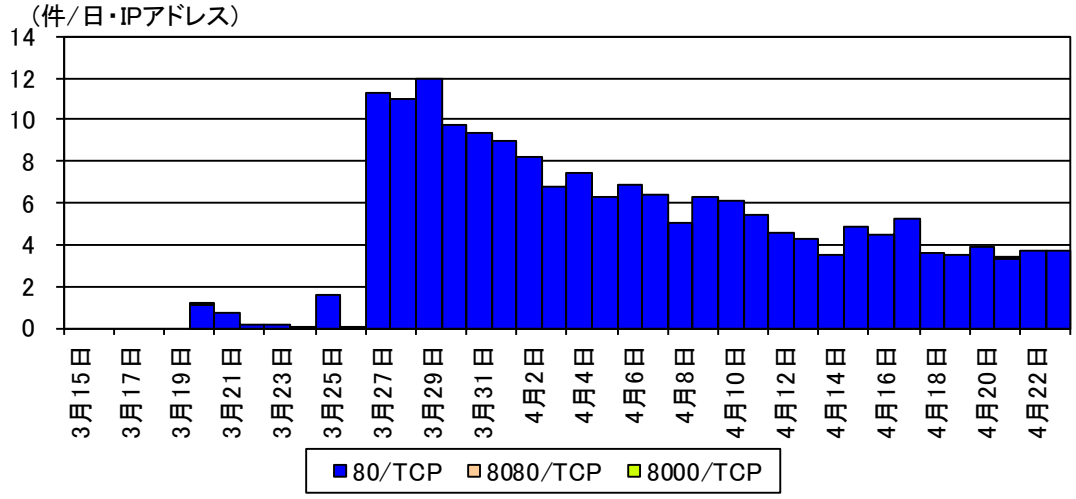

図7　インド製 GPON ルータの脆弱性を悪用したアクセス件数の推移（R2.3.15～R2.4.23）

図8　インド製 GPON ルータの脆弱性を悪用したアクセスの例（一部マスキングを実施）

本脆弱性を悪用するアクセスの送信元 IP アドレスを調査したところ、ルータや IP 電話交換機等の機器のログイン画面が表示されることを確認しました（図9）。

図9　送信元となっている機器のログイン画面の例（一部マスキングを実施）

(4) 台湾製NASに対するリモートコード実行に関する脆弱性 [i] を悪用したアクセスについて、非常に少数ですが観測しています（図 10）。この観測でダウンロードされるプログラムは IoT 機器に感染する「Mirai」の亜種と考えられるものでした。本脆弱性を悪用するアクセスの送信元 IP アドレスについて調査したところ、Android 端末や LTE 通信モジュールに関連するものでした。

図 10　台湾製 NAS の脆弱性を悪用したアクセスの例（一部マスキングを実施）

[i] JVNDB-2020-001758(CVE-2020-0954):
https://jvndb.jvn.jp/ja/contents/2020/JVNDB-2020-001758.html

警察庁では以前にも「複数の IoT 機器等の脆弱性を標的としたアクセスの増加等について」をレポートとして掲載[i]していますが、このように IoT 機器等を標的とした Mirai 亜種をはじめとするマルウェアの感染活動は依然として観測しており、これら機器に対する脅威は継続しています。

IoT 機器等の利用者は、今回の観測との関係の有無に拘ることなく、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。

- 製造元のウェブサイト等で周知される脆弱性情報に注意を払い、脆弱性が存在する場合にはファームウェアのアップデートや、必要な設定変更等の適切な対策を速やかに実施してください。
- 製品によっては、ファームウェアの自動アップデート機能が存在するものもあります。このような製品を使用している場合には、同機能を有効にしてください。
- IoT 機器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せずに、ルータ等を使用してください。
- インターネットからのアクセスを許可する場合は、必要なポートのみに限定してください。また、必要な IP アドレスのみにアクセスを許可したり、VPN を用いて接続したりすることも検討してください。
- 必要がない限りは、ルータの UPnP 機能を無効にしてください。
- ユーザ名及びパスワードは初期設定のままで使用せず、必ず変更してください。また、ユーザ名及びパスワードを変更する際は、推測されにくいものにしてください。
- 製造終了から年月が経過した製品は、製造元のサポートが終了し、脆弱性への対応が実施されない場合があります。そのような製品を使っている場合には、サポート中の製品への更新を推奨します。

[i] 複数の IoT 機器等の脆弱性を標的としたアクセスの増加等について:
https://www.npa.go.jp/cyberpolice/important/2020/202001301.html

2　Microsoft SMBv3 の脆弱性（CVE-2020-0796）に関するアクセスの観測

令和2年3月 13 日に@police の Web サイトにおいて注意喚起[i] を行いましたが、警察庁のインターネット定点観測において、3月 11 日頃から SMBv2 以降のバージョンを確認しているとみられるアクセス(SMB2 NEGOTIATE Request)の増加を観測しました（図 11、図 12）。

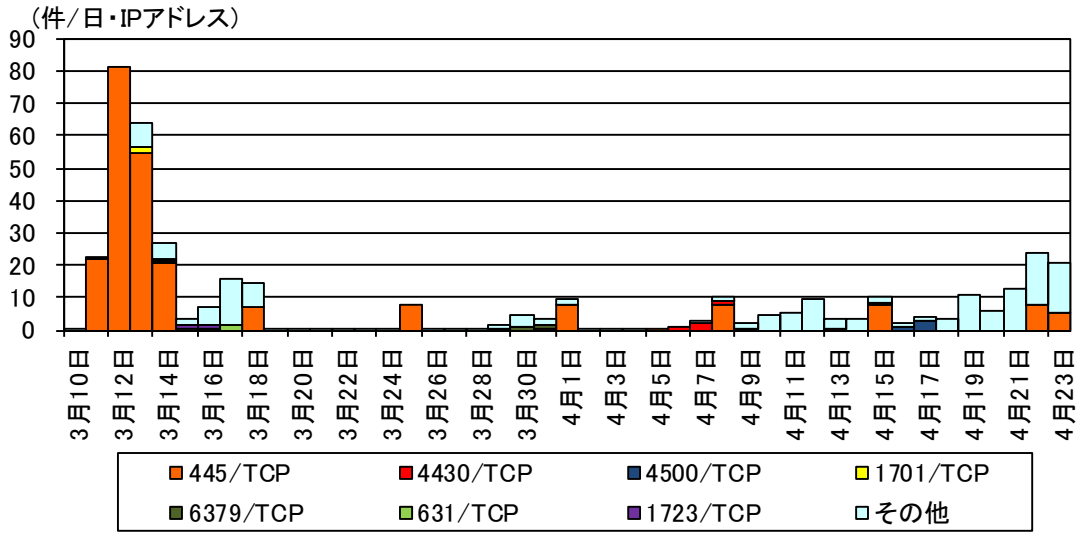

図 11　SMBv2 以降のバージョンを確認しているとみられるアクセス件数の推移
（R2.3.10～R2.4.23）

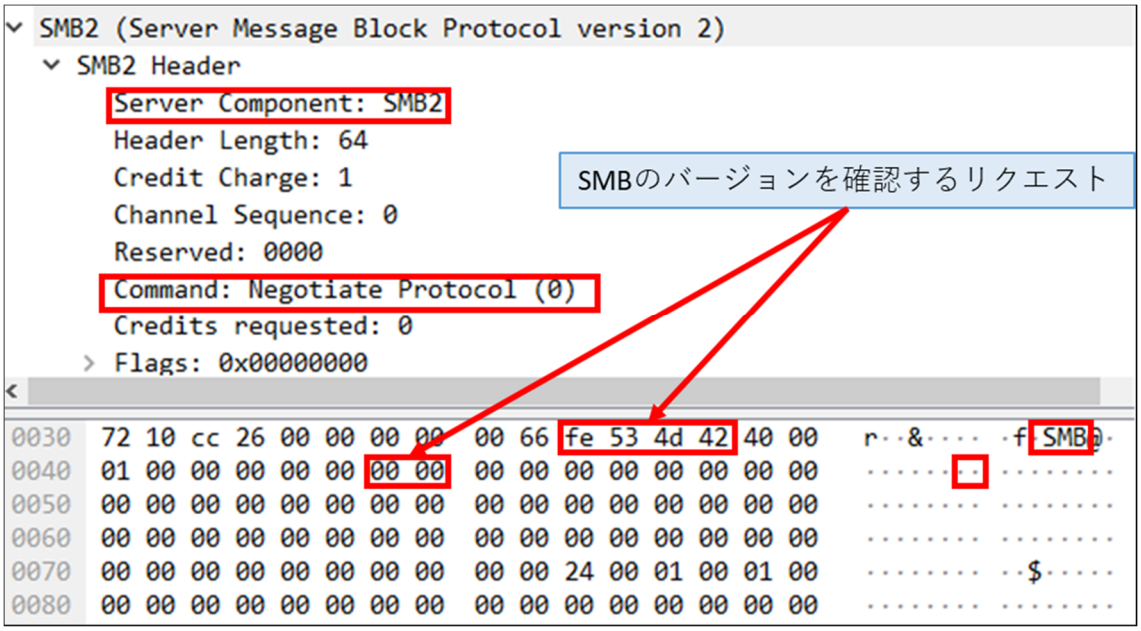

図 12　SMBv2 以降のバージョンを確認しているとみられるアクセスの例

[i] Microsoft SMBv3 の脆弱性（CVE-2020-0796）に関連するアクセスの観測について
https://www.npa.go.jp/cyberpolice/important/2020/202003131.html

Microsoft Server Message Block 3.1.1(SMBv3)には、遠隔から任意のコマンドを実行させることが可能となる脆弱性が公表[i]されています。

3月 12 日にはメモリ破壊をさせることでコンピュータにブルースクリーンを発生させることができる PoC が公開されていることを確認したほか、3月 30 日にはローカル権限昇格の可能性がある PoC の公開を確認しました。

本脆弱性を悪用した攻撃そのものは現時点で確認できていませんが、3月 30 日以降にも、SMBv2 以降のバージョンを確認しているとみられるアクセスを観測しています(図 13)。

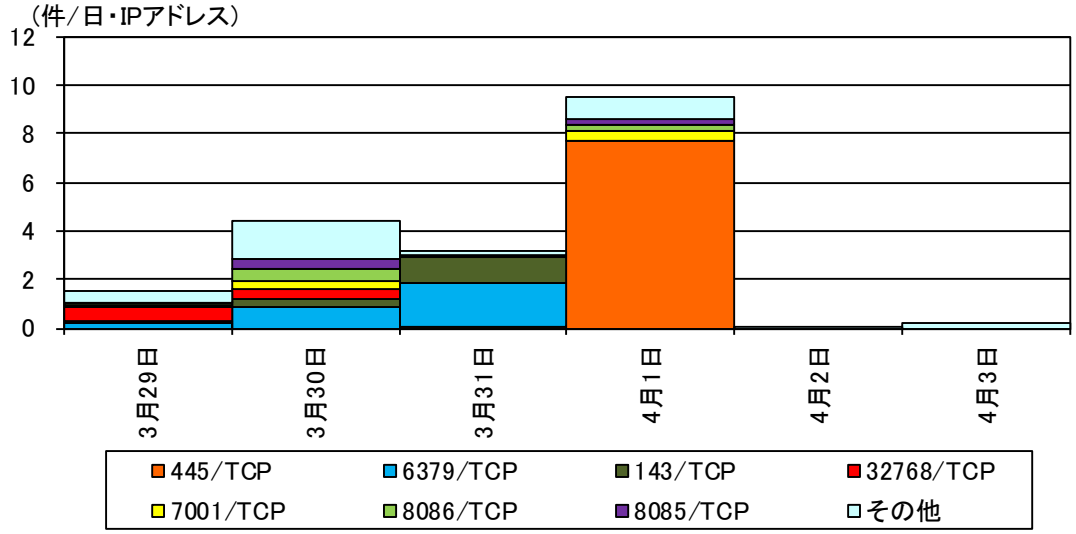

図 13 SMBv2 以降のバージョンを確認しているとみられるアクセス件数の推移
(R2.3.29～R2.4.3)

3月 30 日前後の期間における 445/TCP へのアクセスについては、送信元 IP アドレスを確認すると、そのほとんどが海外のセキュリティ企業や検索サービスによるものでした。445/TCP 以外へのアクセスは、特定の国に割り当てられた[ii]複数の IP アドレスから同じバイト列が送信される調査パケットでした。

これらの送信元 IP アドレスからは本件の他に、SMBv1 など他のサービスが稼働していないかを調査するパケットも送信されています。1週間おきに発生しているアクセスの増加は、これらの調査が定期的に行われていることによるものと思われます。

本脆弱性の対象となるバージョンの Microsoft Windows を利用している場合、以下の対策を早急に実施することを推奨します。

- マイクロソフト社が公開する修正プログラムを適用し、OS を最新の状態にしてください。
- 必要がない場合には、外部からの SMB 接続(445/TCP 等)を遮断することを推奨します。

[i] CVE-2020-0796 | Windows SMBv3 クライアント/サーバーのリモートでコードが実行される脆弱性
https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2020-0796

[ii] 判明した送信元 IP アドレスが当該国・地域に割り当てられていることを指しており、踏み台となっているなどにより、送信者の所在と一致していない場合があります。