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

令和2年7月 16 日

レポート

Microsoft SMBv3 の脆弱性に関するアクセスの観測等について

- Microsoft SMBv3 の脆弱性に関するアクセスの観測
- Liferay Portal の脆弱性を標的としたアクセスの観測

1 Microsoft SMBv3 の脆弱性に関するアクセスの観測

令和2年3月 13 日及び令和2年4月 28 日に@police の Web サイトにおいて注意喚起[i] [ii] を行いましたが、3月 11 日頃から観測されている SMB2 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)は、6月 10 日頃から再び増加しました。(図1)。

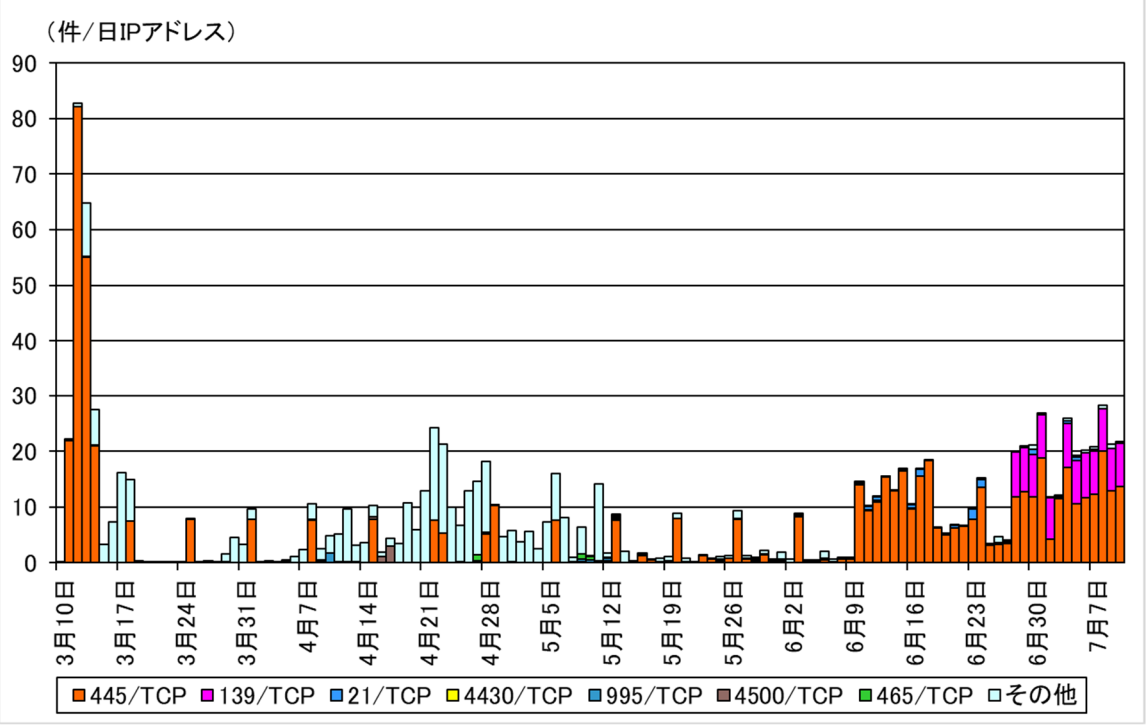

図1 SMBv2 以降のバージョンを確認しているとみられるアクセス件数の推移（R2.3.10～R2.7.10）

[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

[ii] 複数の IoT 機器の脆弱性を悪用したアクセスの観測等について
https://www.npa.go.jp/cyberpolice/important/2020/202004281.html

令和2年3月 13 日に、Microsoft 社から、Microsoft Server Message Block 3.1.1(SMBv3)の遠隔から任意のコマンドが実行可能となる脆弱性に関する情報が公開[i] され、令和2年6月 9 日にも、同社より、Microsoft Server Message Block 3.1.1(SMBv3)における情報漏えいの脆弱性に関する情報が公開[ii] されました。

2種類の脆弱性情報の公開前後より 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が増加しております。

また、当該脆弱性を対象とした探索ツールが海外の共有ウェブサービス上で公開されています。

SMB の脆弱性については、2017 年に流行した Wannacry のように、自動的に感染を広げるマルウェアが作成される可能性があります。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。
- パソコン等をインターネットに接続する場合は、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。
- サーバ等を直接インターネットに接続している場合は、ファイアウォール等を使用して、必要なポートのみを公開することを検討してくだい。
- インターネットからのアクセスを許可する場合には、必要な着信元（送信元）IPアドレスのみにアクセスを許可する、VPNを用いて接続することも検討してください。

[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] CVE-2020-1206 | Windows SMBv3 クライアント/サーバーの情報漏えいの脆弱性
https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2020-1206

2　Liferay Portal の脆弱性を標的としたアクセスの観測

Liferay Portal は Liferay 社製の Web システムを構築するためのオープンソースのソフトウェアです。Liferay Portal は、令和2年3月20日に、遠隔から任意のコードを実行される脆弱性[i]が、公開されています。また、海外の共有ウェブサービスにおいて、当該脆弱性を対象とした PoC[ii]も公開されています。

警察庁のインターネット定点観測において、令和2年4月25日より、当該脆弱性を標的としているとみられるアクセスを観測しています（図2）。

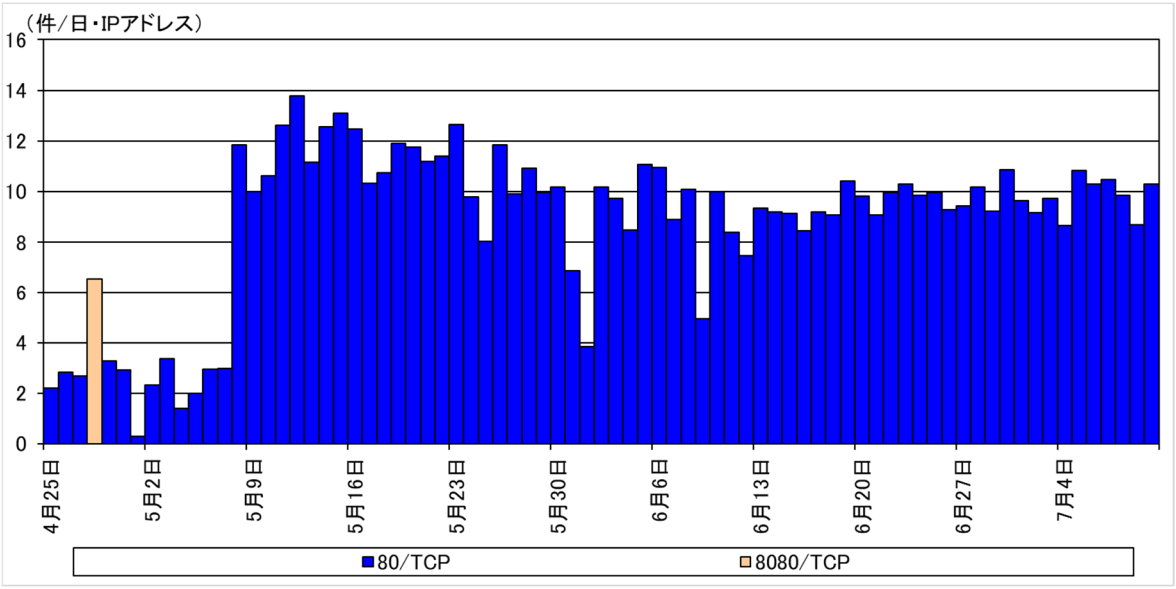

図2　Liferay Portal の脆弱性を標的としたアクセス件数の推移（R2.4.25～R2.7.10）

観測したアクセスは、サーバ内の特定のファイルに対してアクセスを行い、脆弱性の有無を確認するなどの探索行為と思料されます（図3）。

```
POST /api[redacted] HTTP/1.1
Host: [redacted]:80
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Content-Length: 0
Content-Type: application/json
Accept-Encoding: gzip
Connection: close
```

図3　観測したアクセスの例（一部マスキングを実施）

[i] JVNDB-2020-003135(CVE-2020-7961)
https://jvndb.jvn.jp/ja/contents/2020/JVNDB-2020-003135.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。

Liferay Potal の利用者は、バージョンの確認を実施してください。脆弱性のあるバージョンは、以下のとおりです。

- Liferay Potal 7.2 CE GA2 (7.2.1) 未満

使用している Liferay Portal のバージョンが脆弱性の影響を受けるものである場合には、以下の対策を実施してください。

- 開発元から公開されているバージョンへのアップデートを実施してください。
- インターネットからのアクセスを許可する場合には、必要な送信元 IP アドレスのみにアクセスを許可する、VPN を用いて接続することも検討してください。

脆弱性のあるバージョンを使用している場合は、既に攻撃を受けている可能性があります。該当するサーバ等に不審なプロセス、ファイル及び通信等が存在しないか確認してください。