令和２年 10 月 16 日

レポート

vBulletin の脆弱性（CVE-2020-17496）を標的としたアクセスの観測等について

- vBulletin の脆弱性（CVE-2020-17496）を標的としたアクセスの観測
- Android Debug Bridge （ADB）を標的としたアクセスの観測

1 vBulletin の脆弱性（CVE-2020-17496）を標的としたアクセスの観測

vBulletin は MH Sub I LLC.が提供するフォーラムサイトを作成するためのソフトウェアです。令和2年 8 月 10 日、vBulletin に存在する脆弱性（CVE-2020-17496）[i] が公表されました。当該脆弱性は昨年 10 月に「vBulletin の脆弱性(CVE-2019-16759)を標的としたアクセス[ii] 」として@police の Web サイトにおいて注意喚起を行った、遠隔から攻撃者により任意のコードを実行される可能性がある脆弱性の修正を回避する脆弱性です。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[iii] が公開されていることを確認しました。

警察庁のインターネット定点観測において、令和2年8月 14 日以降、当該脆弱性を標的とした宛先ポート 80/TCP 及び 443/TCP に対するアクセスを観測しています（図1）。

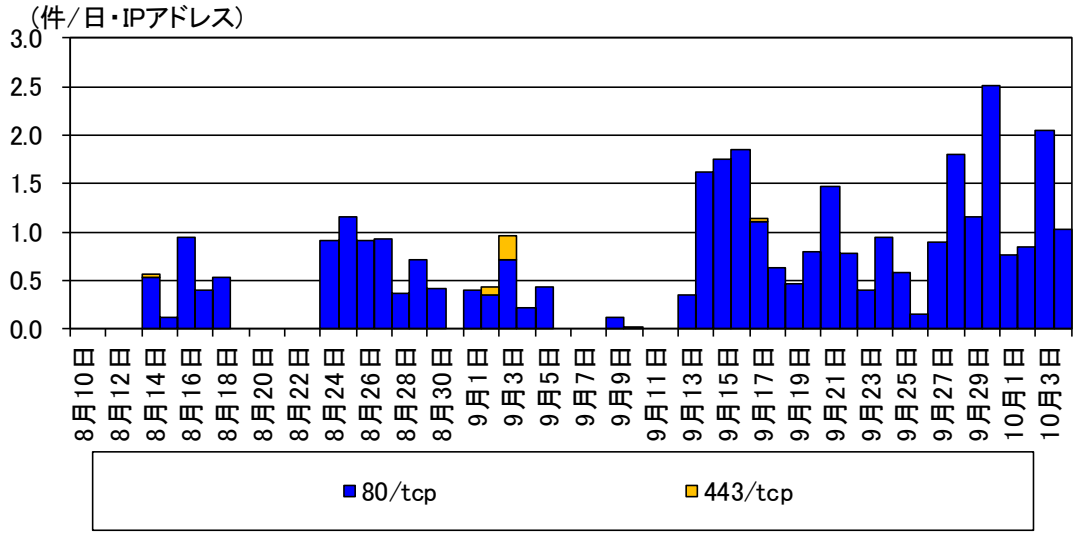

図1 vBulletin の脆弱性（CVE-2020-17496）を標的としたアクセス件数の推移
（R2.8.10～R2.10.4）

[i] NVD-CVE-2020-17496
https://nvd.nist.gov/vuln/detail/CVE-2020-17496

[ii] vBulletin の脆弱性(CVE-2019-16759)を標的としたアクセスの観測等について
https://www.npa.go.jp/cyberpolice/important/2019/201910291.html

[iii] 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。

観測したアクセスは、外部サーバからスクリプトをダウンロードし実行を試みるものでした（図2）。このスクリプトはリバースシェル [i] として動作する perl スクリプトとみられます。

図2　vBulletin の脆弱性（CVE-2020-17496）に対するアクセスの例
（一部マスキングを実施）

vBulletin 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。

- vBulletin 5.5.4 から 5.6.2 のバージョン

使用している vBulletin のバージョンが脆弱性の影響を受けることが判明した場合には、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セキュリティパッチの適用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、通信等が存在しないか確認してください。

[i] 実行された端末から攻撃者端末に接続することで、ファイアウォールなどのネットワーク制御を回避しながらバックドアとして攻撃者からの指令を受け付け、動作するプログラムのこと。

2 Android Debug Bridge（ADB）を標的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、令和2年7月 16 日以降、Android Debug Bridge [i]（ADB）に使用される宛先ポート 5555/TCP に対して、特定のコマンドにより外部サーバからシェルスクリプトをダウンロードし、実行を試みるアクセスの増加を観測しました（図3、4）。

図3 5555/TCP に対する特定のコマンドによるアクセスの例
（一部マスキングを実施）

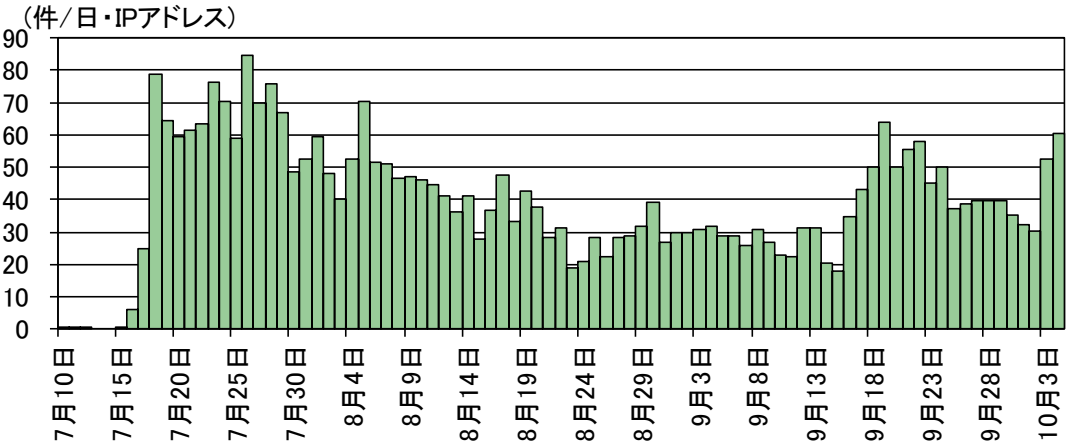

図4 5555/TCP に対する特定のコマンドによるアクセス件数の推移（R2.7.10～R2.10.4）

ダウンロードしたシェルスクリプトが実行されると、外部のサーバから不正プログラムをダウンロードし、実行を試みます。観測により確認の取れたダウンロードされるファイル名とハッシュ値は表1、2のとおりです。これらの不正プログラムは Mirai、又は、その亜種とみられます。

表1 ダウンロードされるファイル名とハッシュ値（8月頃まで）

ファイル名	ハッシュ値（MD5）
bot.aarch64	a8585dd3ff980c91179010e595c20b0b
bot.arm5	a9109419954a421b712d48ea22b0a7b9
bot.arm6	2dabb8e039a77f0eb67e938d798ab7c4
bot.arm7	e2cec25584bfec1e56ee82f350dfeaf9
bot.x86	cc84fcc23567228337e45c9fbb78699f
bot.x86_64	2520fc7d13ac3876cca580791d1c33a8

[i] Android 搭載機器とコンピュータ等を接続しデバッグを行うためのツール。

表2　ダウンロードされるファイル名とハッシュ値（9月以降）

ファイル名	ハッシュ値（MD5）
arm	e2cded792878d91da1501daee113f676
arm5	5cdba55c6480878483bf49fbf534ad8e
arm6	ff6aed0cc372570f5c314a7db2606fd2
arm7	ff6aed0cc372570f5c314a7db2606fd2
m68k	43e7040f08e392367c1e517c3c4d4b9a
mips	7daf2573b7ab4a16ade2a341d67a03bd
mpsl	0462ca44fd0734f0c03012addcb32482
ppc	da54b2616e669e98c4dfb3642a55bf35
sh4	ed273b9046db78cec8ca69f80b6bf41b
x86	dfe3993296bbd498edeb13db05966494

また、不正プログラムをダウンロードさせる外部のサーバについては、本年8月に「ZeroShellの脆弱性を標的としたアクセスの観測について[i]」として@police の web サイトにおいて注意喚起を行っていますが、こちらで観測された不正プログラムをダウンロードさせる外部のサーバと同じIP アドレスのサーバでした。ADBを標的としたアクセスについては、8月中旬頃にダウンロードさせる外部サーバの IP アドレスが変化し、9 月には別の IP アドレスのものも確認しています。参考に同期間の ZeroShell の脆弱性を標的としたアクセス件数の推移を示しますが（図5）、いずれのアクセスの上昇も7月 16 日から顕著になっています。

なお、これらのアクセスについては宛先 IP アドレスと TCP シーケンス番号[ii] の初期値が一致する Mirai ボットの特徴はみられませんでした。

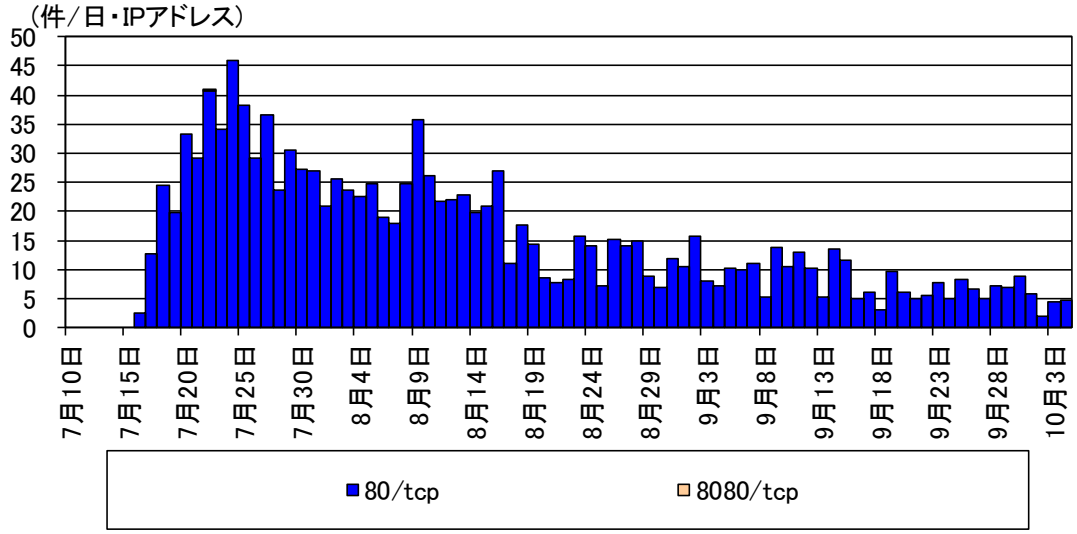

図5　ZeroShell の脆弱性を標的としたアクセス件数の推移（R2.7.10～R2.10.4）

[i] ZeroShell の脆弱性を標的としたアクセスの観測について
https://www.npa.go.jp/cyberpolice/important/2020/202008111.html

[ii] TCP パケットの送受信状況を管理するための番号で、通常は TCP 通信の開始時にランダムな番号が初期値として設定され、進行に合わせて増加します。また、この初期値を特に ISN（Initial Sequence Number）といいます。

これらのことから、ZeroShell の脆弱性を標的とした不正プログラムの配信インフラと、宛先ポート 5555/TCP を使用している Android 搭載機器を標的とした不正プログラムの配信インフラが、Mirai、又は、その亜種といった IoT 機器に感染する不正プログラムを配信するためのものとして共有されていることがうかがえます。

これまでも@police の web サイトでは、IoT 機器等を標的としたアクセスの観測について注意喚起を行っておりますが、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。これらの機器の利用者は、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。