令和元年10月29日

レポート

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

- vBulletinの脆弱性(CVE-2019-16759)を標的としたアクセスの観測について
- WS-Discoveryに応答する機器を標的とした探索活動の観測について

1 vBulletinの脆弱性(CVE-2019-16759)を標的としたアクセスの観測について

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。令和元年9月24日、vBulletinに存在する深刻な脆弱性(CVE-2019-16759)[i]が公表されました。当該脆弱性が悪用された場合、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ります。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]が公開されています。

警察庁のインターネット定点観測においては、令和元年9月25日以降、当該脆弱性を標的とした宛先ポート80/tcpに対するアクセスを観測しています(図1)。

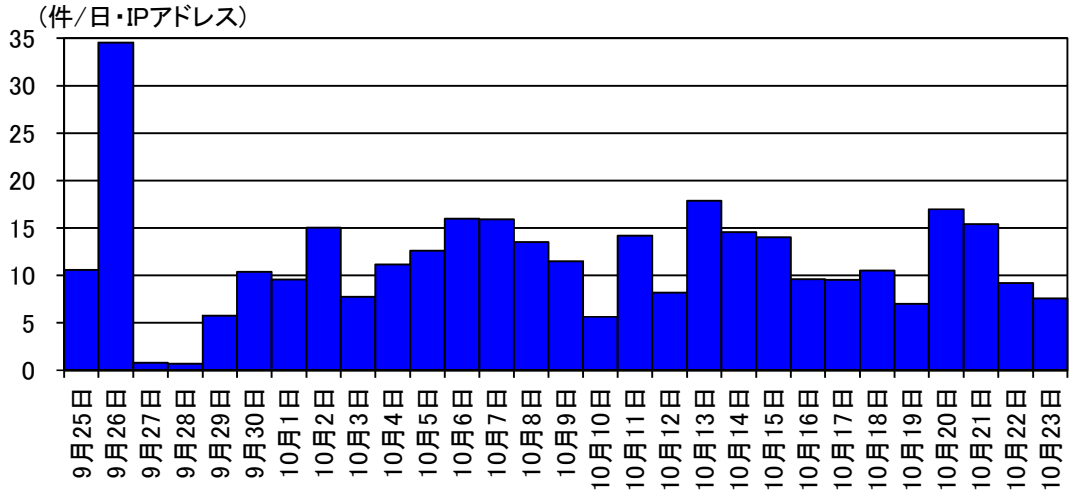

図1 vBulletinの脆弱性(CVE-2019-16759)を標的とした宛先ポート80/tcpに対するアクセス件数の推移(R1.9.25～10.23)

観測したアクセスの中には、当該脆弱性を悪用し、サーバ内の特定ファイルを改ざんする行為が含まれていました(図2)。この改ざんは、遠隔から被害サーバに任意のコードを実行させる際に、特定の文字列(パスワード)を必要とする仕組みを組み込むものであり、他の攻撃者の利用を制限するためのものと見られます。

[i] 「CVE-2019-16759 Detail」
https://nvd.nist.gov/vuln/detail/CVE-2019-16759

[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。

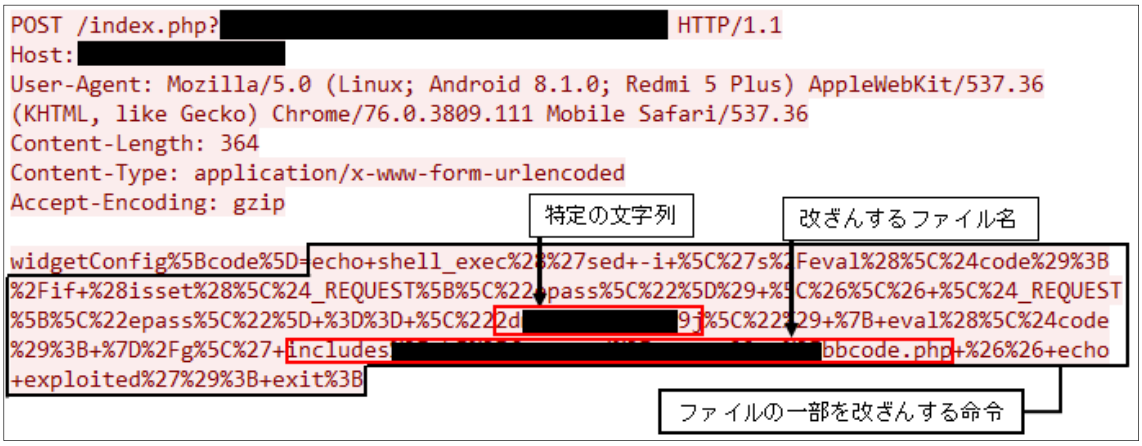

図2　特定ファイルを改ざんするアクセスの内容（一部マスキングを実施）

9月 27 日より、改ざん行為によって組み込まれた特定文字列によるコード実行機能の有無を確認しているとみられるアクセス（アクセス1）を観測しました（図3）。ただし、確認に用いる送信データが不完全なものであったため確認に失敗していたと推測されます。

図3　アクセス1の内容（一部マスキングを実施）

しかし、10 月 10 日からは、送信データを修正したアクセス（アクセス2）が観測されるようになりました（図4）。

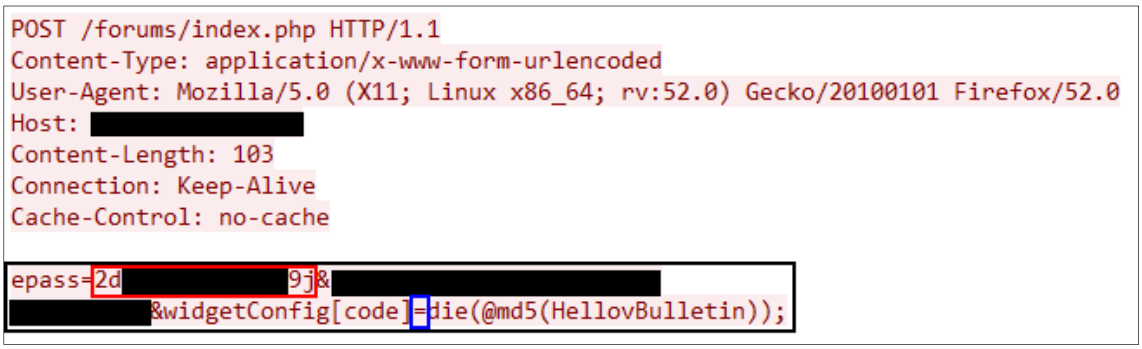

図4　アクセス2の内容（一部マスキングを実施）

観測した vBulletin の脆弱性を標的としたアクセスの推移（図1）のうち、改ざん有無を確認しているとみられるアクセス件数の推移は図5のとおりとなっています。

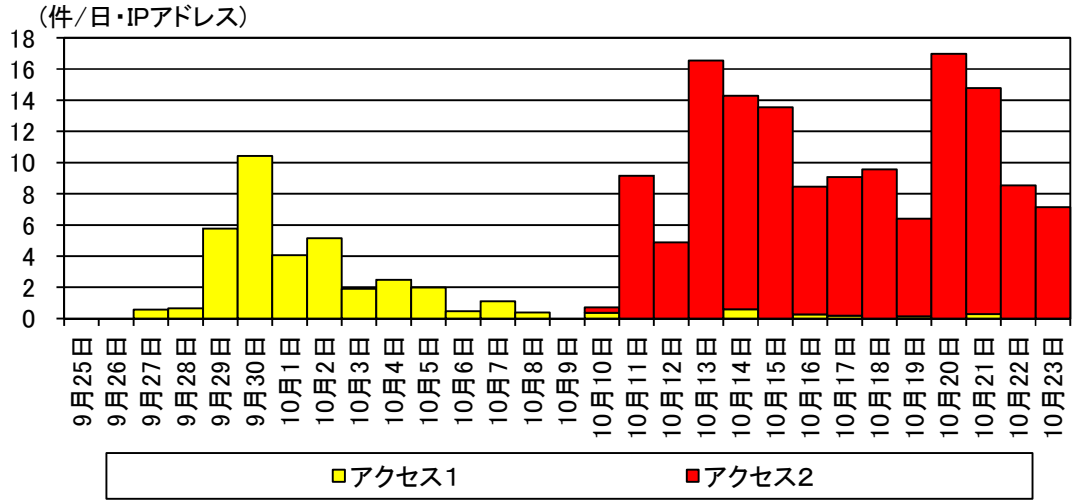

図5　改ざん有無を確認しているとみられるアクセス件数の推移
（R1.9.25～10.23）

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 5.0.0 から 5.5.4 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。

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。

２　WS-Discovery に応答する機器を標的としたアクセスの観測について

警察庁のインターネット観測において、令和元年8月頃から WS-Discovery で使用する、宛先ポート 3702/UDP に対するアクセスの増加を観測しました（図6）。WS-Discovery は、ローカルネットワーク上のネットワークカメラやプリンター等のデバイスを検出するために使用されるプロトコルです。

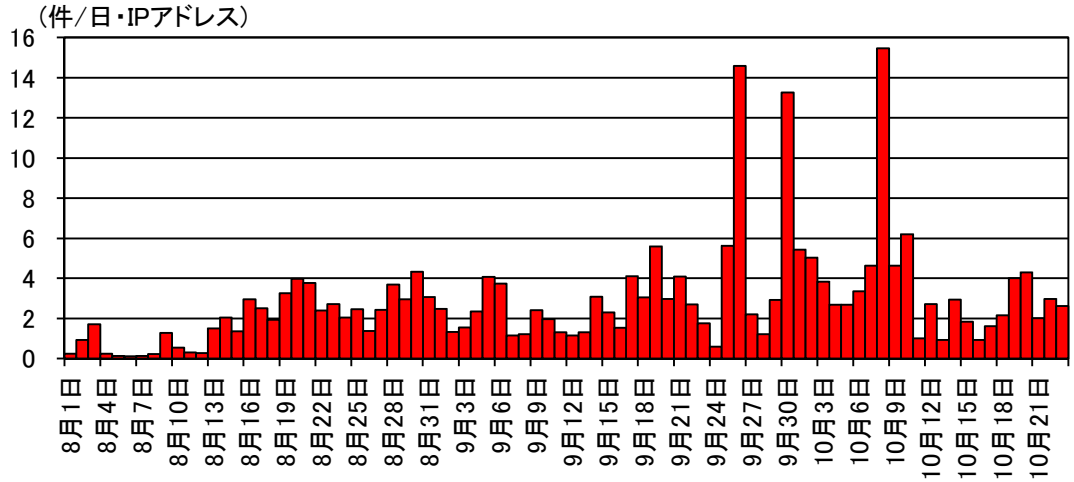

図6　宛先ポート 3702/UDP に対するアクセス件数の推移（R1.8.1～10.23）

通常、WS-Discovery はローカルネットワーク内で使用されることを想定したプロトコルですが、機器の設定不備により、インターネット上からの当該プロトコルに対するアクセスに応答する機器が存在しています。また、WS-Discovery を UDP プロトコルで使用する場合、着信元（送信元）IP アドレスの偽装が容易であるという UDP プロトコルの特性から、攻撃先となる機器に対して偽装した UDP パケットを大量に送ることが可能となり、DDoS 攻撃の踏み台に悪用されてしまう可能性があります。観測したアクセス内容を確認したところ、DDoS 攻撃に悪用可能な WS-Discovery に応答する機器の探索行為とみられるアクセスを観測しました（図7、図8）。

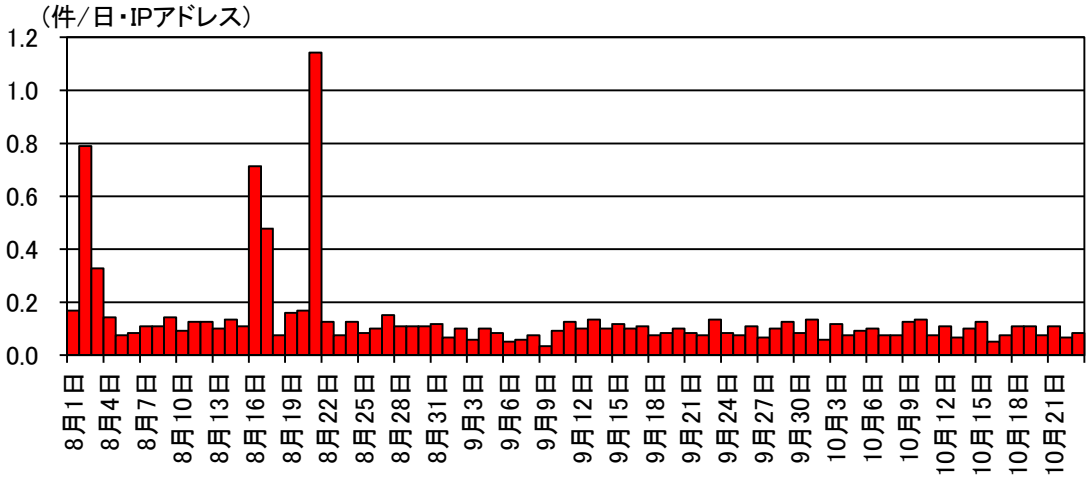

図7　WS-Discovery に応答する機器の探索行為と見られるアクセス件数の推移
（R1.8.1～10.23、宛先ポート 3702/udp）

<?xml version="1.0" encoding="UTF-8"?><s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://schemas.xmlsoap.org/ws/2004/08/addressing"><s:Header><a:Action s:mustUnderstand="1">http://schemas.xmlsoap.org/ws/2005/04/discovery/Probe</a:Action><a:MessageID>[redacted]</a:MessageID><a:ReplyTo><a:Address>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</a:Address></a:ReplyTo><a:To s:mustUnderstand="1">urn:schemas-xmlsoap-org:ws:2005:04:discovery</a:To></s:Header><s:Body><Probe xmlns="http://schemas.xmlsoap.org/ws/2005/04/discovery"><d:Types xmlns:d="http://schemas.xmlsoap.org/ws/2005/04/discovery" xmlns:dp0="http://www.onvif.org/ver10/network/wsdl">dp0:NetworkVideoTransmitter</d:Types></Probe></s:Body></s:Envelope>

図8　観測したアクセスの例（一部マスキングを実施）

WS-Discovery を使用した DDoS 攻撃の事例について、令和元年 8 月に海外のセキュリティ企業である zeroBS [i] 社が報じています。

また、WS-Discovery に応答する機器に対して意図的に細工したパケットが送信された場合、応答した機器の IP アドレスやモデル番号が漏洩する可能性があります [ii]。これらの情報から応答した機器の脆弱性が新たに判明した場合、当該機器の脆弱性を介して内部ネットワークへ侵入される可能性があります。

管理する機器が攻撃の踏み台として悪用される、あるいはその他の脆弱性から内部ネットワークに侵入されないために、以下の対策を実施することを推奨します。

- FW やルータ等で、WS-Discovery を使用する機器のポート（3702/UDP）に対するインターネットからのアクセスを遮断してください。
- 管理する機器が、WS-Discovery を使用してインターネットへアクセスを行わない設定になっていることを確認してください。

[i] 「New DDoS Attack-Vector via WS-Discovery/SOAPoverUDP, Port 3702」
https://zero.bs/new-ddos-attack-vector-via-ws-discoverysoapoverudp-port-3702.html

[ii] 「NEW DDOS VECTOR OBSERVED IN THE WILD: WSD ATTACKS HITTING 35/GBPS」
https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html