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

令和２年６月５日

レポート

# Zyxel CNM SecuManager の脆弱性を標的としたアクセスの観測等について

- Zyxel CNM SecuManager の脆弱性を標的としたアクセスの観測
- Hadoop YARN ResourceManager の脆弱性を標的としたアクセスの観測
- Symantec Web Gateway の脆弱性を標的としたアクセスの観測

## １　Zyxel CNM SecuManager の脆弱性を標的としたアクセスの観測

Zyxel CNM SecuManager は Zyxel 社製のネットワーク機器を管理するソフトウェアです。令和2年3月 13 日、Zyxel CNM SecuManager の複数の脆弱性に関する情報が、Zyxel 社より公開[i]されました。それらの情報には、遠隔から攻撃者により任意のコードを実行される脆弱性が存在していました。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4月 12 日以降、当該脆弱性を標的とした宛先ポート 9673/TCP に対するアクセスを観測しています（図1）。

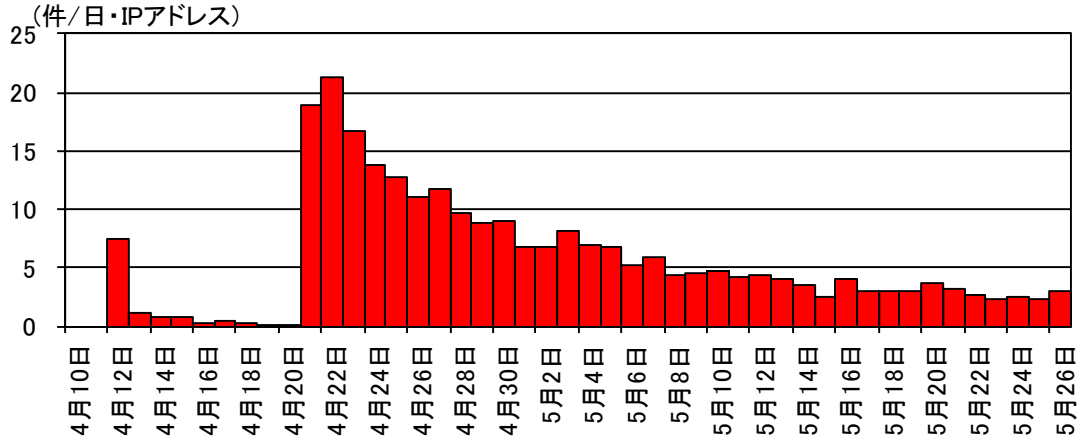


図１　Zyxel CNM SecuManager の脆弱性を標的とした宛先ポート 9673/TCP に対するアクセス件数の推移（R2.4.10～R2.5.26）

観測したアクセスは、当該ソフトウェアの脆弱性を利用して、任意のコードを実行させるものでした（図2）。

[i] Zyxel security advisory for vulnerabilities of CloudCNM SecuManage
https://www.zyxel.com/support/vulnerabilities-of-CloudCNM-SecuManager.shtml

[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。

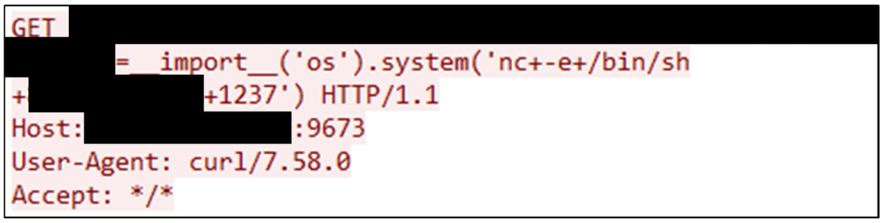


図2　Zyxel CNM SecuManager の脆弱性に対するアクセスの例1（一部マスキングを実施）

また、4月 13 日以降のアクセスは、任意のコードを実行することで、不正プログラムのダウンロード及び実行を試みるアクセスへと変化しています（図3）。


図3　Zyxel CNM SecuManager の脆弱性に対するアクセスの例2（一部マスキングを実施）

当該脆弱性について、Zyxel 社は修正中であり、当該脆弱性が解決次第、利用者に連絡すると発表しています。

## 2 Hadoop YARN ResourceManager の脆弱性を標的としたアクセスの観測

Hadoop は、大規模データの蓄積・分析を実現するオープンソースのミドルウェアです。Hadoop YARN ResourceManager とは、 Hadoop がクライアントから実行データを受け取るプログラムです。海外の共有ウェブサービスにおいて、Hadoop YARN ResourceManager には、遠隔から攻撃者により任意のコードを実行される脆弱性が存在し、当該脆弱性を対象とした PoC 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4月 16 日以降、当該脆弱性を悪用するために必要となるデータの取得を試みるアクセスの増加を観測しました（図4）。

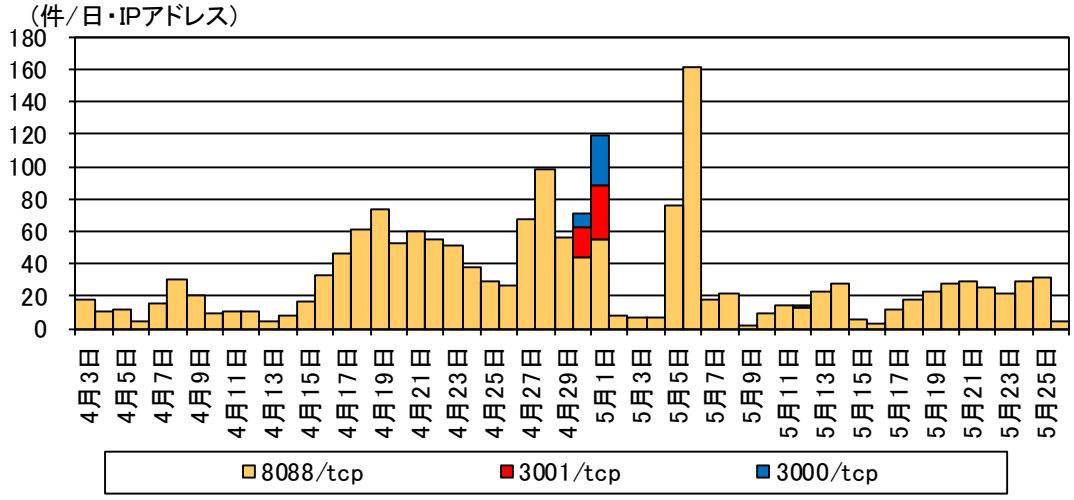


図4 Hadoop YARN ResourceManager の脆弱性を悪用するために必要となるデータの取得を試みるアクセスの件数の推移（R2.4.3～R2.5.26）

観測したアクセスは、当該脆弱性を悪用するために必要となるデータの取得を試みるもので、脆弱性のある Hadoop YARN ResourceManager の探索行為が行われていると考えられます（図5）。

```
POST [redacted] HTTP/1.1
Host: [redacted]:8088
User-Agent: Go-http-client/1.1
Content-Length: 0
Connection: close
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
```

図5 Hadoop YARN ResourceManager の脆弱性を悪用するために必要となるデータの取得を試みるアクセスの例（一部マスキングを実施）

図5のアクセスによりHadoopから得られるデータと、当該脆弱性を悪用することにより、Hadoopのサーバ内で任意のコードを実行することが可能です。

内部システムに Hadoop を使用している場合には、以下の対策を実施することを推奨します。

- 内部システムへアクセスできないようにファイアウォールやルータの設定を変更してください。
- 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 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。
- 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。

## 3　Symantec Web Gateway の脆弱性を標的としたアクセスの観測

Symantec Web Gateway は、各種セキュリティ対策に利用される Symantec 社のアプライアンス製品です。令和2年3月 27 日に、海外の共有ウェブサービスにおいて、Symantec Web Gateway には、リモートコード実行の脆弱性が存在し、当該脆弱性を対象とする PoC が公開されていることを確認しました。この脆弱性が悪用された場合、遠隔で任意のコードを実行される可能性があります。警察庁のインターネット定点観測において、当該脆弱性を標的としたアクセスを 4 月 25 日より観測しています（図6）。

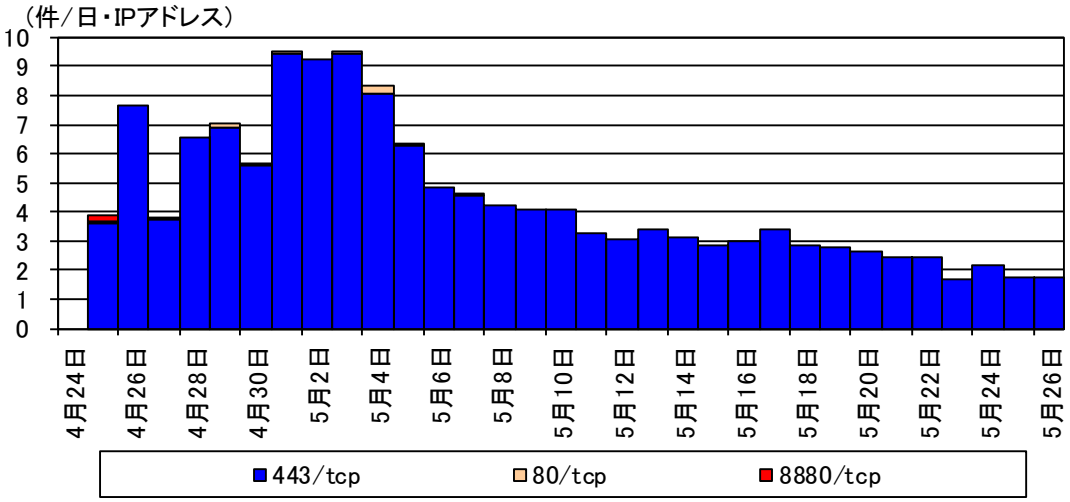


図6　Symantec Web Gateway の脆弱性を標的としたアクセス件数の推移
（R2.4.24～R2.5.26）

観測されたアクセスは、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（図7）。


図7　Symantec Web Gateway 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）

公開された PoC の情報によると、脆弱性のあるバージョンは、以下のとおりです。

- Symantec Web Gateway 5.0.2.8

使用している Symantec Web Gateway 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。

- 脆弱性のあるバージョンは、最新のバージョンではないことから、製造元の情報を確認し、更新することを検討してください。
- 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。