Ksisnetだより
発行:Ksisnet事務局
令和 4年 1月 24日
Vol.102

脆弱性対策情報の公開に伴う悪用増加

「情報セキュリティ10大脅威2021(組織編)」で、「脆弱性対策情報の公開に伴う悪用増加」が第10位にランクインしています。2022年も、引き続き注意しておく必要があります。

ソフトウェアの脆弱性対策情報の公開は、脆弱性の脅威や対策情報を広く呼びかけられるメリットがある一方、その情報を攻撃者に悪用され、当該ソフトウェアに対する脆弱性対策を行っていないシステムを狙った攻撃が行われています。

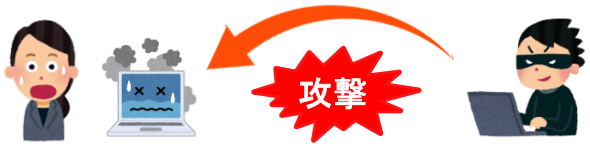
<攻撃手口>

1 対策前の脆弱性(Nデイ脆弱性)を悪用

ソフトウェアに脆弱性が発見され、セキュリティパッチパッチが公開されても、適用するまでには いくらかの時間がかかります。このセキュリティパッチが適用されるまでの時間に存在する脆弱性をNデイ脆弱性といい、システムで使用しているソフトウェアの管理が不適切だとこの時間が長くなり、被害に遭うおそれが大きくなります。

2 公開されている攻撃ツールを悪用

公開された脆弱性に対する攻撃ツールは短期間で作成され、ダークウェブ上のウェブサイト等で販売されることがあります。また、オープンソースのツールに脆弱性を利用する機能が実装され、それを悪用されることもあります。

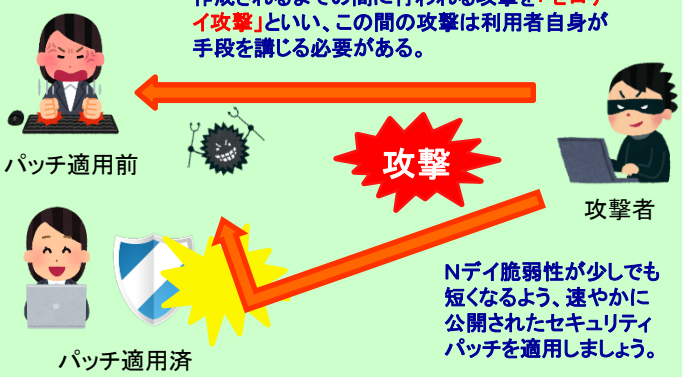


<脅威と影響>

ソフトウェアに脆弱性が発見された場合、当該ソフトウェアの開発ベンダー等が、脆弱性を修正するためのセキュリティパッチを作成し、公開して、当該ソフトウェアの利用者へ対策を促します。

一方攻撃者は、脆弱性が見つかると攻撃するためのマルウェアを開発し、パッチを適用していない利用者に対して脆弱性を悪用した攻撃を行います。

昨今、脆弱性が発見されてから、それを悪用した攻撃が発生するまでの期間が短くなっており、より迅速な対応が求められています。



<対策/対応>

個人、組織(システム管理者/ソフトウェア利用者)

- 被害の予防
  - 情報セキュリティ対策の基本を実施
  - 資産の把握、体制の整備
  - 脆弱性関連情報の収集と対応
  - UTM、IDS/IPS、WAF等の外部からの攻撃等を防御するシステムの導入
    導入後も対策情報を定期的に更新する
  - ネットワークの監視および攻撃通信の遮断
  - セキュリティのサポートが充実しているソフトウェアを使う
    パッチの提供が早い等のサポートが充実したものを選ぶ
  - 一時的なサーバの停止
    すぐにパッチが適用できない場合、一時的にサーバ停止等を実施して、攻撃を回避する対策も検討する
- 被害を受けた後の対応
  - CSIRT等所定の連絡先への連絡
  - 影響調査および原因の追究、対策の強化

組織(開発ベンダー)

- 製品セキュリティの管理、対応体制の整備
  - 製品に組み込まれているソフトウェアの把握、管理の徹底
  - 脆弱性関連情報の収集
  - 脆弱性発見時の対応I手順の作成
    情報を迅速に発信できる仕組みの整備

参考 IPA(情報処理推進機構)