滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R４年度 No. 8
今、注目のサイバーセキュリティに関する情報をお届けします。

脆弱性の対策できていますか？

サイバー攻撃の１つに脆弱性（ぜいじゃくせい）が悪用されるという手口があります。
ランサムウェア攻撃についても、VPNの脆弱性を突かれているものが発生しています。
脆弱性とは、プログラム上の不備です。脆弱性は、機器のファームウェアも含めてソフトウェアの更新や修正プログラムの適用で防ぐことができます。
脆弱性が発見された場合は、早急に対策を実施するようにしましょう。

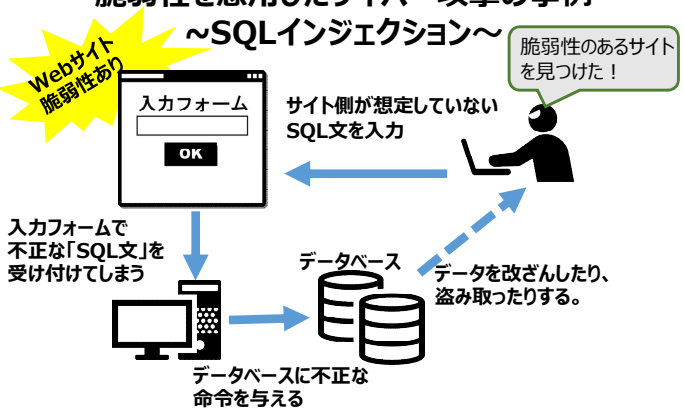
脆弱性とは

「脆弱」というのは、もろくて弱いという意味ですが、コンピュータの世界でいう脆弱性は、プログラム上の不備や欠陥のことをいいます。
プログラムは、コンピュータに対する命令を記述したもので、プログラムを組み合わせたものがソフトウェアとなります。プログラムは非常に複雑で不備なく完璧に作成することは困難と言われています。
ですから、ソフトウェアは、提供後も脆弱性が見つかると、修正しながら利用していく仕組みとなっています。

ゼロデイ攻撃

脆弱性が公になってから、メーカー等がその穴を塞ぐための修正プログラムを提供するまでの期間に行われる攻撃を、ゼロデイ攻撃と言います。この期間に攻撃を受けると、防ぐ手段はないため、利用者自身が「避ける手段」を講じる必要があります。

脆弱性を悪用したサイバー攻撃の事例 ～SQLインジェクション～



SQLとは、データベース内の情報を取得・検索するデータベース言語です。脆弱性のあるWebサイトのフォームに「SQLの断片」としてコンピュータが認識できる文字列を入力することで、不正にデータベースの内容を削除したり、本来アクセスできない情報へのアクセスが可能になったりします。（この場合の脆弱性は、不正なSQL文を受け付けてしまう状態をいいます。） SQLインジェクションを防ぐには、不正なSQL文を回避するプログラムが必要です。

脆弱性情報（緊急性、重要性の高い脆弱性情報等をピックアップしてご紹介します。）

～マイクロソフト社の月例更新プログラムについて～
マイクロソフト製品は、毎月第２週ころに、「月例更新プログラム」が発表されています。
緊急性や重要性が高い脆弱性（放置すると攻撃を受けるおそれが高いもの）を中心に修正プログラムが提供されますので、必ず、更新するようにしましょう。**「自動更新」設定が推奨されます。**
詳細は、必ず、公式サイト及びIPA、JVN、JPCERT/CC等の脆弱性情報提供サイトを確認してください。

サービス名、機器名（影響を受けるソフトウェア）	脆弱性の概要（悪用された場合の影響等）	CVE（共通脆弱性識別子）	対策（修正プログラムの公開情報等）
Windows8.1,10,11 WindowsServer MicrosoftOffice　等	リモートで任意のコードが実行される可能性がある等	CVE-2022-22047　等	更新プログラムの適用 （７月の月例セキュリティ更新プログラムに含まれている）

参照：JPCERT/CC「2022年７月マイクロソフトセキュリティ更新プログラムに関する注意喚起」 https://www.jpcert.or.jp/at/2022/at220018.html

«Emotetの新たな手口に注意»
Emotetに感染すると、Webブラウザ「Google Chrome」に保存されていたクレジットカード情報等が盗まれ、外部に送信される場合があることが確認されています。
メールの添付ファイルを開くときは、十分注意してください。
「コンテンツの有効化」ボタンは安易に押さないようにしましょう。

«CS情報SHIG@»不正アクセスに注意。多要素認証や二段階認証を利用しましょう。

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）　詳細は県警webページで →