サイバーセキュリティ通信 Vol.18

令和5年2月

サイバァちゃん

「VMware ESXi」のぜい弱性 今、狙われています！

欧米を中心に「VMware ESXi」の既知のぜい弱性（CVE-2021-21974）を悪用したランサムウェア「ESXiArgs」の被害が多発しています。
日本国内においても、同様の被害が発生したことから、今一度、自社の機器について確認してください。

＜ぜい弱性情報＞

既知のOpenSLPのヒープオーバーフローのぜい弱性（CVE-2021-21974）

リモートから認証なしで任意のコードを実行され、プログラムの実行、異常終了、該当コンピュータに保存されているデータの改ざん・削除・漏えい等を行われる恐れがあります。

＜対象製品・バージョン＞

・VMware ESXi 7.0系　Update 1cより前のバージョン
・VMware ESXi 6.7系　ESXi670-202102001より前のバージョン
・VMware ESXi 6.5系　ESXi650-202102001より前のバージョン
・VMware Cloud Foundation 4系 4.2より前のバージョンに含まれるESXi
・VMware Cloud Foundation 3系 KB82705未適用のバージョン含まれるESXi

※令和3年2月以降にセキュリティ更新プログラムが適用されていないもの

＜推奨対策＞

・製品を最新のバージョンに更新してください。
サポート対象外のバージョンを使用している場合は、サポート対象のバージョンへ移行してください。

・稼働するサービスやアクセス制限を見直ししてください。
インターネットからESXiサーバに意図せず接続可能となっていないかを確認してください。
OpenSLPサービスを利用していない場合は、無効化してください。

被害に遭われた際は

警察に相談してください。

長崎県警察本部生活安全部サイバー犯罪対策課
095-820-0110（3451・3452）

公式LINEアカウントで
情報配信中！