VMware製品でのLog4Shell悪用

Apache Log4jの脆弱性「Log4Shell」は2021年12月に公表されたものですが、未だ攻撃者によって悪用され続けており、CISA(米国サイバーセキュリティ・インフラセキュリティ庁)は、2022年6月、7月と2回にわたって、Log4Shellを利用した「VMware Horizon」や「VMware Unified Access Gateway(UAG)」への攻撃について注意喚起しています。

VMware Horizon、UAGには Log4jが含まれており、その脆弱性に対処していない場合、攻撃の対象となりかねないので、VMware Horizon、UAGを最新のバージョンへのアップデートするなどの対策を講じてください。

脆弱性通称 : Log4Shell

共通脆弱性識別子: CVE-2021-44228

対象: Apache Log4i-core 2.15.0 より前の2系

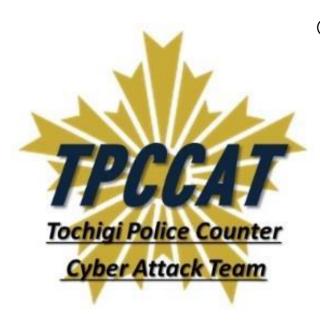
バージョン

脆弱性の概要 : Apache Log4jが稼働するサーバに、第三者

が脆弱性を悪用するデータを送信して、任意

のコードを実行する可能性がある

共通脆弱性評価 : 10(緊急)



○ Log4Shellに限らず、攻撃者は古い脆弱性もサイバー攻撃に利用するので、機器やソフトウェアのアップデートを欠かさず行うようにしてください。

