2021年12月14日

お客様各位

株式会社日立ソリューションズ
Fortinet製品ユーザサポート

Apache Log4jの脆弱性(CVE-2021-44228)のFortinet製品への影響について

拝啓、平素は Fortinet 製品サポートをご利用下さいまして誠にありがとうございます。

先日、ApacheのJavaベースのログ出力ライブラリである「Apache Log4j」について、脆弱性情報(CVE-2021-44228)が公開されています。当該脆弱性に関するFortinet製品への影響を下記にご案内します。

敬具

記

1. CVE-2021-44228のFortinet製品への影響

当サポートサイトで取り扱っている、以下製品はCVE-2021-44228の影響を受けません。

詳細については、Fortinet社から発表されているPSIRT Advisories(*1)をご覧ください。

尚、同サイト記載内容以上の情報は開示されていません。記載内容の解釈また記載内容以上の情報については、弊社サポートではお答えいたしかねます。予めご了承ください。

・FortiOS (FortiGate および FortiWiFi)
・FortiAnalyzer
・FortiManager
・FortiAP

2. IPSシグネチャでの対応状況

本脆弱性への対応したIPSシグネチャ(Apache.Log4j.Error.Log.Remote.Code.Execution)をIPSパッケージ version 19.215以降で、VID 51006としてリリースされています。

なお、シグネチャによる誤検知防止の観点から、当該シグネチャの新規リリース(version 19.215)時点では、検知時の既定のアクションは通信を許可する設定となっています。version 19.215で通信を制限するには、検知時のアクションをBlockにするなどの設定が必要です。

2021年12月14日現在で最新のversion 19.217では、検知時のデフォルトのアクションはBlockに変更されています。

以上

(*1) Apache log4j2 log messages substitution (CVE-2021-44228)
https://www.fortiguard.com/psirt/FG-IR-21-245