Apache Log4j における複数の脆弱性(Log4shell)の影響について

公開日 2022 年 3 月 29 日
三菱電機株式会社

■概要

Java ロギングフレームワーク Apache Log4j において、設計上の欠陥に起因する複数の脆弱性が、公開されました。これらの脆弱性を悪意のある攻撃者に悪用された場合、対象製品において、情報漏えいやサービスの停止(DoS)が発生したり、悪意のあるプログラムが実行される可能性があります。本脆弱性の影響を受ける製品名を以下に示しますので、対策又は軽減策・回避策の実施をお願いいたします。

■CVSS スコア

CVE-2021-44228(CWE-502):	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	基本値:10.0
CVE-2021-45046(CWE-502):	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	基本値: 9.0
CVE-2021-45105(CWE-20,674):	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	基本値: 5.9

■脆弱性の説明

Apache Log4j においてログメッセージを十分に入力検証せずに処理して、実行してしまう問題により、情報漏えい、サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性が存在します。
当社製品は、下記脆弱性の影響を受ける可能性があります。「■影響を受ける製品、対策方法及び軽減策・回避策」に、製品毎に影響を受ける可能性がある脆弱性の番号(1～3)を掲載しますので、ご確認ください。

1. 十分にログメッセージの検証を行わずに、JNDI※においてログメッセージを処理することによる、悪意のあるプログラムが実行される脆弱性(CVE-2021-44228)(CWE-502)
2. CVE-2021-44228 に対する修正が不十分であり、特定の条件下で、十分にログメッセージの検証を行わずに、JNDI においてログメッセージを処理することによる、悪意のあるプログラムが実行される脆弱性(CVE-2021-45046)(CWE-502)
3. 再帰的(self-referential)な Lookup 処理における不十分な入力検証及び不適切な再帰処理の制御による、サービス拒否(DoS)の脆弱性(CVE-2021-45105)(CWE-674、CWE-20)

※･･･Java Naming and Directory Interface の略。Java で標準的に利用される API の一種で、ディレクトリサービスなどにアクセスする標準的なインターフェース仕様を定義したもの。

■脆弱性がもたらす脅威

攻撃者によって何らかの方法で細工された文字列をログファイルへ出力したとき、情報漏えいやサービスの停止(DoS)が発生したり、悪意のあるプログラムが実行される可能性があります。

■影響を受ける製品、対策方法及び軽減策・回避策

[1]【CC-Link IE TSN マスタ・ローカル局通信 LSI (CP610)用設定ツール CC-Link IE TSN Configurator】

型番	対策及び軽減策・回避策
SW1DNN-GN610SRC-M 上記製品の Ver.1.02C 以前の全てのバージョンが影響を受ける可能性があります (1、2、3 の影響を受ける可能性があります)	＜想定される影響＞ 本製品がインストールされたコンピュータに対して、悪意のある攻撃者に、これらの脆弱性を悪用された場合、情報漏えい及びサービスの停止(DoS)の発生並びに悪意のあるプログラムが実行される可能性があります。 ＜対策＞ 以下サイトより Ver.1.12F 以降をダウンロードしたうえで、アップデートしてください。 https://www.mitsubishielectric.co.jp/fa/download/index.html ＜アップデート方法＞ 1. ダウンロードしたファイル(zip 形式)を解凍します。 2. 解凍されたフォルダの中の「SW1DNN-GN610SRC-M.exe」を実行します。インストール先に指定したフォルダにファイルが展開されます。 3. "CCLinkIE_TSN_configuration_tool"フォルダに格納されている"Tools.exe"を実行すると CC-Link IE TSN Configurator が Tools フォルダ内に展開されます。 ＜軽減策・回避策＞ すぐに本製品をアップデート出来ない場合、以下に示す軽減策を講じることを推奨します。 ・本製品をインストールしたコンピュータをインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止してください。

●お客様からのお問い合わせ先

製品をご購入いただいた当社の支社、代理店にご相談ください。

<お問い合わせ | 三菱電機 FA>
https://www.mitsubishielectric.co.jp/fa/support/purchase/index.html