2022 年 4 月 5 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

Spring Framework の脆弱性(CVE-2022-22965)および Spring Cloud Function の脆弱性(CVE-2022-22963)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、Java の「Spring Framework」および「Spring Cloud Function」について、脆弱性情報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-2022-22965(通称：Spring4Shell)および CVE-2022-22963 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-2022-22965 および CVE-2022-22963 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

それぞれの脆弱性への IPS シグネチャでの対応状況は以下となります。

(1) CVE-2022-22965

本脆弱性(CVE-2022-22965)に対応した IPS シグネチャが IPS パッケージ version 20.287 以降で、VID 51352 としてリリースされています。(*2)

尚、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 20.287)

(*1) CVE-2022-22965 and CVE-2022-22963 vulnerabilities
https://www.fortiguard.com/psirt/FG-IR-22-072

(*2) Spring.Framework.SerializationUtils.Insecure.Deserialization
https://www.fortiguard.com/encyclopedia/ips/51352

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。また、2022 年 4 月 4 日現在で最新の version 20.289 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。このため、version 20.289 未満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。

(2) CVE-2022-22963

本脆弱性(CVE-2022-22963)に対応した IPS シグネチャが IPS パッケージ version 20.289 以降で、VID 51355 としてリリースされています。(*3)

尚、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 20.289)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 20.289 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。

以上

(*3) Spring.Cloud.Function.Routing.Expression.Remote.Code.Execution
https://www.fortiguard.com/encyclopedia/ips/51355