２０２２年４月８日

お客様各位

株式会社日立ソリューションズ
Palo Alto Networks 製品ユーザーサポート

Spring Framework の脆弱性(CVE-2022-22963, CVE-2022-22965)について

平素は Palo Alto Networks 製品ユーザーサポートをご利用くださいまして誠にありがとうございます。この度、Palo Alto Networks 社より、Spring Framework の脆弱性についてアナウンスされましたので、以下の通りご連絡いたします。

1. 概要

Palo Alto Networks 社は、Spring Cloud Function の脆弱性(CVE-2022-22963)および Spring Core の脆弱性(CVE-2022-22965)について調査を行っています。
2022 年 4 月 8 日時点では、Palo Alto Networks 社製品およびサービスはこれらの脆弱性の影響を受けないことが確認されております。

2. 対象のお客様

2022 年 4 月 8 日時点では、Palo Alto Networks 社製品およびサービスにおいて本脆弱性の影響を受ける製品はございません。

3. 対応シグネチャ

PA シリーズの脅威防御機能にて CVE-2022-22963, CVE-2022-22965 の検知/遮断が可能となる、脆弱性防御シグネチャがリリースされております。各シグネチャの情報と内包されているコンテンツバージョンは下記の表 3.1 の通りです。

表 3.1 CVE-2022-22963, CVE-2022-22965 の検出と遮断に必要なシグネチャ情報

Threat ID	CVE	Severity	Default-Action	First Release	Last Update
92389	2022-22963	critical	reset-server	8548-7321	8550-7325
92393	2022-22965	critical	reset-server	8548-7321	8551-7330
92394	2022-22965	critical	reset-server	8548-7321	8550-7325

(2022 年 4 月 8 日時点)

※コンテンツは随時アップデートされており、今後新たな対応シグネチャがリリースされることや、既存のシグネチャが更新される可能性もございますので、コンテンツバージョンを最新に保つことをご検討ください。

4. その他特記事項

本脆弱性の詳細や最新情報については、下記の Palo Alto Networks 社ページも併せてご参照ください。

Security Advisories
CVE-2022-22963 Informational: Impact of Spring Vulnerabilities CVE-2022-22963 and CVE-2022-22965
https://security.paloaltonetworks.com/CVE-2022-22963

なお、掲載されている以上の情報は開示されておりません。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致しかねますことを予めご了承ください。

また、Palo Alto Networks 社からは、2022 年 3 月 9 日および同 31 日に本脆弱性以外にも Palo Alto Networks 社製品に関するセキュリティアドバイザリーが複数発表されております。（High 1 件、Medium 1 件、None 2 件）
これらについても上記の Security Advisories からご参照ください。

以上