サイバーセキュリティ通信 Vol.16

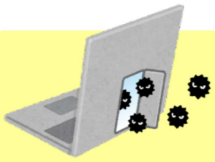
令和5年２月

サイバァちゃん

ぜい弱性情報について

Fortinet製品及びSophos製品ついて、ぜい弱性が確認されています。
これらの製品については**既に攻撃に利用された事例もあります**ので、**該当する製品を利用していないか確認**し、利用がある場合は製品各社が公開している**更新プログラムの適用**を行ってください。

Fortinet製品 「FortiOS」



バッファオーバーフローのぜい弱性を悪用することで、認証資格を持たない攻撃者が細工したリクエストを送信し、遠隔で任意のコード・コマンドを実行できる可能性がある（CVE-2022-42475）

＜対象製品・バージョン＞
FortiOS：v7.2.0～7.2.2、v7.0.0～7.0.8、v6.4.0～6.4.10、v6.2.0～6.2.11、
v6.0.0～6.0.15、v5.6.0～5.6.14、v5.4.0～5.4.13、v5.2.0～5.2.15
v5.0.0～5.0.14
FortiOS-6K7K：v7.0.0～7.0.7、v6.4.0～6.4.9、v6.2.0～6.2.11、v6.0.0～6.0.14

更新プログラムの適用がどうしてもできない場合・・・

SSL-VPN機能を **無効** にしてください。

対象機器があった場合は下記についても確認してください

- 機器ログにぜい弱性の悪用を示すログが記録されていないか
- 機器に不審なファイルが設置されていないか
- 機器から不審な通信先への通信が発生していないか

※詳しい内容については、Fortinetが提供する情報を確認してください。

【参考】Fortinet「FortiOS-heap-based buffer overflow in sslvpnd」
https://www.fortiguard.com/psirt/FG-IR-22-398

Sophos製品 「Sophos Firewall」

- コードインジェクションのぜい弱性により、リモートコード実行ができる可能性がある（CVE-2022-3236）
- OSコマンドインジェクションのぜい弱性、管理者がSSL-VPN設定のアップロードを介してコード実行できる可能性がある（CVE-2022-3226）
- コードインジェクションのぜい弱性、隣接する攻撃者がWi-fiコントローラでコード実行できる可能性がある（CVE-2022-3713）
- コードインジェクションのぜい弱性、管理者がWebadminでコード実行できる可能性がある（CVE-2022-3696）
- XSSのぜい弱性、管理者からスーパー管理者権限への昇格を可能とする可能性がある（CVE-2022-3709）
- SQLインジェクションのぜい弱性、ユーザが機密性の低い設定のデータベースコンテンツを読み取ることができる可能性がある（CVE-2022-3711）
- SQLインジェクションのぜい弱性、APIクライアントが機密性の低い設定のデータベースコンテンツを読み取ることができる可能性がある（CVE-2022-3710）

＜対象製品・バージョン＞
Sophos Firewall　v19.0 MR1（19.0.1）　およびそれ以前

【参考】Sophos 「Sophos Firewall v19.5 GA Resolves Security Vulnerabilities」
https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0

もし被害に遭われた際は……

警察にご相談ください。

長崎県警察本部生活安全部サイバー犯罪対策課
095-820-0110（3451・3452）

公式LINEアカウントで
情報配信中！