ルータファームウェアに隠れているサイバー攻撃者に関するレポート

アドバイザリーID : cisco-sa-csa-cyber-report-sept-2023
初公開日 : 2023-09-27 13:50
最終更新日 : 2023-09-27 18:19
バージョン 1.2 : Final
回避策 : No workarounds available
Cisco バグ ID :

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

2023年9月27日、米国国家安全保障局(NSA)、米国連邦捜査局(FBI)、米国サイバーセキュリティおよびインフラストラクチャセキュリティ機関(CISA)、警察庁(NPA)、およびサイバーセキュリティに関する全米問題準備および戦略センター(NISC)は、サイバー攻撃者の活動を詳述した共同サイバーセキュリティアドバイザリ(CSA)を発表しました。

このレポートの詳細については、「中華人民共和国がリンクしたサイバー攻撃者がルータファームウェアに隠れる」を参照してください。

シスコはレポートを確認しました。シスコは次の重要な事実を強調したいと考えています。

- これらの攻撃で最も一般的な初期アクセスベクトルは、盗まれたり、脆弱な管理者クレデンシャルが含まれます。このレポートで概説されているように、ロギングの無効化やファームウェアのダウンロードなどの特定の設定変更には、管理者クレデンシャルが必要です。
- シスコの脆弱性が悪用された形跡はありません。攻撃者は、侵害されたクレデンシャルを使用して、管理レベルの設定とソフトウェアの変更を実行しました。
- 最新のシスコデバイスには、修正されたソフトウェアイメージのロードと実行を許可しないセキュアブート機能が含まれています。セキュアブートの詳細については、『Cisco Trustworthy Technologies Data Sheet』を参照してください。
- レポートに記載されている盗まれたコード署名証明書は、シスコからのものではありません。シスコは、シスコインフラストラクチャデバイスに対する攻撃を実行するために盗まれたコード署名証明書に関する知識を持っていません。

これらのキーポイントは、シスコの一貫した姿勢とメッセージに沿ったものであり、シスコのブログ記事「攻撃者はレガシーデバイスを狙い続ける」に記載されているベストプラクティスに従

うようお客様に助言します。

最新のネットワークインフラストラクチャデバイスには、前述の攻撃を軽減する多数のセキュリティ機能が搭載されています。Cisco Secure Development Lifecycle(SDL)は、業界をリードするプラクティスとテクノロジーを適用して、現場で発見された製品セキュリティインシデントが少ない、信頼できるソリューションを構築します。ネットワークの信頼性に対する継続的な取り組みの一環として、シスコは最近、ネットワークの耐障害性に重点を置いた取り組みを開始しました。この取り組みの詳細については、Cisco Network Resilienceポータルを参照してください。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csa-cyber-report-sept-2023

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csa-cyber-report-sept-2023

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	明確化を追加。	要約	Final	2023年9月27日
1.1	調整された書式。	要約	Final	2023年9月27日
1.0	初回公開リリース	—	Final	2023年9月27日

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。