# Cisco Secure Firewall Adaptive Security Appliance(ASA)およびSecure Firewall Threat Defenseに対する持続性メカニズムの継続的な進化


アドバイザリーID : cisco-sa-asaftd-persist-CISAED25-03
初公開日 : 2026-04-23 15:00
最終更新日 : 2026-04-24 13:37
バージョン 1.1 : Final
回避策 : No workarounds available
Cisco バグ ID : CSCwt61597

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

2026年4月23日、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庁(CISA)は、V1:Emergency Directive(ED)25-03: Identify and Allowance of Cisco Devices related to Cisco Secure Firewall Adaptive Security Appliance(ASA)およびCisco Secure Firewall Threat Defense(FTD)製品に関するアップデートを発行しました。

今回の更新により、ArcaneDoorの脅威担当者は、2025年9月に公開された修正済みリリースへのアップグレードを通じて維持される、未知の持続性メカニズムを開発しました。この持続性メカニズムは、該当するハードウェアプラットフォーム上のCisco Secure Firewall ASAソフトウェアおよびCisco Secure FTDソフトウェアのインストール用のCisco Firepower eXtensible Operating System(FXOS)ソフトウェアベースオペレーティングシステムにあります。

注：Cisco PSIRTがこれまでに受け取った情報によると、最初のセキュリティ侵害は、2025年9月に入手可能になった修正済みリリースにお客様がアップグレードする前に、攻撃者が次の脆弱性を悪用することから始まります。

- CVE-2025-20333:Cisco Secure Firewall適応型セキュリティアプライアンスソフトウェアおよびSecure Firewall Threat DefenseソフトウェアのVPN Webサーバにおけるリモートコード実行の脆弱性
- CVE-2025-20362:Cisco Secure Firewall適応型セキュリティアプライアンスソフトウェアおよびSecure Firewall Threat DefenseソフトウェアのVPN Webサーバの不正アクセスの脆弱

性

2025年9月にリリースされた修正済みリリースの詳細については、『シスコイベントレスポンス：シスコファイアウォールに対する継続的な攻撃』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-asaftd-persist-CISAED25-03

# 詳細

詳細については、Cisco TalosブログのUAT-4356's Targeting of Cisco Firepower Devicesを参照してください。

# セキュリティ侵害の痕跡

新しく発見された持続性インプラントは、lina_csという悪意のあるプロセスを開始することが知られています。このプロセスが存在するかどうかを確認するには、デバイスでshow kernel process | include lina_csコマンドを使用します。次の例に示すように、show kernel process | include lina_csコマンドによって何らかの出力が返された場合、そのデバイスは侵害を受けたと見なされます。

Cisco SecureファイアウォールASA

```
<#root>

asa#

show kernel process | include lina_cs

68081 29428  20   0      249856      100        1    S     3     0    0

lina_cs
```

シスコセキュアFTD

```
<#root>

 >

show kernel process | include lina_cs

 68081 29428  20   0      249856      100        1    S     3     0    0

lina_cs
```

注：lina_csプロセス名はインプラントの設計によって異なる可能性があるため、このセクションのIndicators of Compromise(IOC)では持続性インプラントを最終的に特定できない場合があります。

緩和策についての詳細は、このアドバイザリの「回避策」セクションを参照してください。

## 回避策

持続性メカニズムを完全に削除するには、このアドバイザリの「修正済みソフトウェア」セクションに記載されている修正済みリリースを使用してデバイスを再イメージングし、アップグレードすることを強く推奨します。詳細については、特定の製品の再イメージングのマニュアルを参照してください。

- Cisco Secure Firewall ASAおよび脅威対策の再イメージングガイド
- Firepower 4100および9300シリーズのFXOSで完全な再イメージ化を実行する
- 1000、2100、および3100シリーズのセキュアFTDの再イメージ化

このアドバイザリの「修正済みソフトウェア」セクションに記載されている修正済みリリースにイメージを再適用し、アップグレードすることを推奨します。

Cisco Secure ASAまたはFTDプラットフォームで侵害が確認された場合、デバイスのすべての構成要素を信頼できないと見なす必要があります。すべての設定（特にローカルパスワード、証明書、および鍵）を再設定し、すべての証明書および鍵を再生成することを推奨します。

代替緩和（非推奨）:次の操作を行うことで、再イメージングが可能になるまでこの問題を緩和できます。

コールドリスタートを行うと、悪意のある永続インプラントが取り除かれます。shutdown、reboot、およびreloadの各CLIコマンドでは、悪意のある固定インプラントはクリアされません。電源コードを抜いて、デバイスに差し込む必要があります。

重要：デバイスの電源を切断すると、データベースやディスクが破損する危険性があり、デバイスが期待どおりに起動または実行されない可能性があります。このため、侵害が疑われる場合は、デバイスのイメージを再作成することを強く推奨します。

## 修正済みソフトウェア

次の表では、左の列にシスコソフトウェアトレインを示します。右の列は、各ソフトウェアトレインの最初の修正済みリリースを示しています。

このアドバイザリの「侵害の痕跡」のセクションで概説したように、デバイスの侵害が確認された場合、次の修正済みリリースのいずれかを使用して、デバイスのイメージを再作成し、アップグレードする必要があります。

Cisco Secure Firewall ASA ソフトウェア

| Cisco Secure Firewall ASAソフトウェアコードトレイン | First Fixed Release（修正された最初のリリース） |
|---|---|
| 9.16 | 9.16.4.92 |
| 9.18 | 9.18.4.135 |
| 9.20 | 9.20.4.30 |
| 9.22 | 9.22.3.5 |
| 9.23 | 9.23.1.195 |
| 9.24 | 9.24.1.155 |

Cisco Secure FTD ソフトウェア

| Cisco Secure FTDソフトウェアコードトレイン | First Fixed Release（修正された最初のリリース） |
|---|---|
| 7.0 | 7.0.9の後にホットフィックスFZ-7.0.9.1-3が続く<br><br>Cisco_FTD_Hotfix_FZ-7.0.9.1-3.sh.RE L.tar<br>Cisco_FTD_SSP_FP1K_Hotfix_FZ-7.0.9.1-3.sh.RE L.tar<br>Cisco_FTD_SSP_FP2K_Hotfix_FZ-7.0.9.1-3.sh.RE L.tar<br>Cisco_FTD_SSP_Hotfix_FZ-7.0.9.1-3.sh.RE L.tar |
| 7.2 | 7.2.11に続いてホットフィックスHI-7.2.11.1-1<br><br>Cisco_FTD_Hotfix_HI-7.2.11.1-1.sh.RE L.tar<br>Cisco_FTD_SSP_FP1K_Hotfix_HI-7.2.11.1-1.sh.RE L.tar<br>Cisco_FTD_SSP_FP2K_Hotfix_HI-7.2.11.1-1.sh.RE L.tar<br>Cisco_FTD_SSP_FP3K_Hotfix_HI-7.2.11.1-1.sh.RE L.tar<br>Cisco_FTD_SSP_Hotfix_HI-7.2.11.1-1.sh.RE L.tar |
| 7.4 | 7.4.7 |
| 7.6 | 7.6.4に続いてホットフィックスCC-7.6.4.1-1<br><br>Cisco_FTD_Hotfix_CC-7.6.4.1-1.sh.RE L.tar<br>Cisco_FTD_SSP_FP1K_Hotfix_CC-7.6.4.1-1.sh.RE L.tar<br>Cisco_FTD_SSP_FP3K_Hotfix_CC-7.6.4.1-1.sh.RE L.tar<br>Cisco_FTD_SSP_Hotfix_CC-7.6.4.1-1.sh.RE L.tar<br>Cisco_Secure_FW_TD_4200_Hotfix_CC-7.6.4.1-1.sh.RE L.tar |
| 7.7 | 7.7.11に続いてホットフィックスAE-7.7.11.1-4 |

| Cisco Secure FTDソフトウェアコードトレイン | First Fixed Release（修正された最初のリリース） |
|---|---|
| | Cisco_FTD_Hotfix_AE-7.7.11.1-4.sh.RE L.tar<br>Cisco_FTD_SSP_FP1K_Hotfix_AE-7.7.11.1-4.sh.RE L.tar<br>Cisco_FTD_SSP_FP3K_Hotfix_AE-7.7.11.1-4.sh.RE L.tar<br>Cisco_FTD_SSP_Hotfix_AE-7.7.11.1-4.sh.RE L.tar<br>Cisco_Secure_FW_TD_4200_Hotfix_AE-7.7.11.1-4.sh.RE L.tar |
| 10.0 | 10.0.0の後にホットフィックス（2026年4月30日目標） |

これらのホットフィックスのダウンロード方法およびインストール方法の詳細については、『Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes』を参照してください。

Firepower 4100および9300セキュリティアプライアンス

| Cisco Firepower 4100および9300セキュリティアプライアンス | First Fixed Release（修正された最初のリリース） |
|---|---|
| 2.10 | 2.10.1.383 |
| 2.12 | 2.12.1.117 |
| 2,14 | 2.14.3.125 |
| 2.16 | 2.16.2.119 |
| 2.17 | 2.17.0.549 |
| 2.18 | 2.18.0.535 |

注：Cisco Firepower 4100および9300セキュリティアプライアンスの場合、Cisco FXOSコードトレインのダウンロードに関する情報は、『Cisco Firepower 4100/9300 FXOS互換性』を参照してください。

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

## 不正利用事例と公式発表

Cisco PSIRTでは、この問題が活発に悪用されていることを認識しています。

## 出典

シスコは、この調査における米国の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)の協力に感謝いたします。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| 1.1 | セキュリティ侵害の指標を簡素化し、回避策に関する情報を追加。 | 侵入の痕跡と回避策 | Final | 2026年4月24日 |
| 1.0 | 初回公開リリース | — | Final | 2026年4月23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。