Cisco Secure Firewall適応型セキュリティアプライアンスおよびSecure Firewall Threat Defenseソフトウェアの SAML反映クロスサイトスクリプティングの脆弱性

Medium

アドバイザリーID : cisco-sa-asaftd-saml-LktTrwZP
初公開日 : 2026-03-04 16:00
バージョン 1.0 : Final
CVSSスコア : 6.1
回避策 : No workarounds available
Cisco バグ ID : CSCwp29401

CVE-2026-20102

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

Cisco Secure Firewall ASAソフトウェアおよびCisco Secure Firewall Threat Defense(FTD)ソフトウェアのSAML 2.0シングルサインオン(SSO)機能の脆弱性により、認証されていないリモート攻撃者がSAML機能に対してクロスサイトスクリプティング(XSS)攻撃を実行し、ブラウザベースの機密情報にアクセスできる可能性があります。

この脆弱性は、複数のHTTPパラメータの不十分な入力検証に起因します。攻撃者は、悪意のあるリンクにアクセスするようにユーザを誘導することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は該当デバイスを介してリフレクトされたXSS攻撃を実行できる可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありません。

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-saml-LktTrwZP

このアドバイザリは、2026年3月に公開された『Cisco Secure Firewall ASA、Secure FMC、およびSecure FTDソフトウェアセキュリティアドバイザリバンドル』の一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: March 2026 Semiannual Cisco Secure Firewall ASA, Secure FMC, and Secure FTD Software Security Advisory Bundled Publication』を参照して

ください。

該当製品

脆弱性のある製品

この脆弱性が公開された時点では、シスコデバイスで脆弱性のあるCisco Secure Firewall ASAソフトウェアまたはSecure FTDソフトウェアのリリースが実行されており、Internet Key Exchangeバージョン2(IKEv2)またはリモートアクセスSSL VPN機能がSAML 2.0 SSOで設定されている場合に、シスコデバイスに影響が及びました。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

Cisco Secure ASAソフトウェアおよびセキュアFTDソフトウェア設定の確認

Cisco Secure Firewall ASAソフトウェアおよびSecure FTDソフトウェアは、次の機能がすべて設定されている場合にのみ、この脆弱性の影響を受けます。

- SAML 2.0 Identity Provider（IdP）
- SAML 2.0 Service Provider（SP）
- リモート アクセス VPN

ソフトウェアにSAML 2.0 IdPが設定されているかどうかを確認するには、show webvpn saml idp CLIコマンドを使用します。次の出力は、SAML 2.0 IdPで設定されたCisco Secure Firewall ASAソフトウェアを示しています。

```
<#root>

ciscoasa#

show webvpn saml idp

 saml idp

my_domain_idp


url sign-in

 https://asa-dev.my.domain.com/idp/endpoint/HttpRedirect
  url sign-out https://asa-dev.my.domain.com/idp/endpoint/HttpRedirect


trustpoint idp

 my_domain_trustpoint
  trustpoint sp asa_trustpoint
```

ソフトウェアにSAML 2.0 SPが設定されているかどうかを確認するには、show running-config tunnel-group | include remote-access|webvpn-attributes|saml CLIコマンドを使用します。次の出力は、SAML 2.0 SPで設定されたCisco Secure Firewall ASAソフトウェアを示しています。

```
<#root>

ciscoasa#

show running-config tunnel-group | include remote-access|webvpn-attributes|saml


tunnel-group cloud_idp_onelogin

type remote-access


tunnel-group cloud_idp_onelogin webvpn-attributes


authentication saml
 saml identity-provider

my_domain_idp
```

ソフトウェアにリモートアクセスVPNが設定されているかどうかを確認するには、show running-config CLIコマンドを使用し、脆弱性のある設定について次の表を参照してください。

機能	脆弱性の存在するコンフィギュレーション
IKEv2リモートアクセスVPN	`crypto ikev2 enable <interface_name>`
SSL VPN	`webvpn` ` enable <interface_name>`

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が Cisco Secure Firewall Management Center（FMC）ソフトウェアには影響を与えないことを確認しました。

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェア

お客様が Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアにおける脆弱性のリスクの有無を判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。 また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。すべてのアドバイザリ、セキュリティへの影響の評価（SIR）が「重大」または「高」のアドバイザリのみ、またはこのアドバイザリのみを選択します。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco Secure Firewall ASA ソフトウェアの場合は 9.20.3.4、Cisco Secure FTD ソフトウェアの場合は 7.4.2 と入力します。
5. [チェック（Check）] をクリックします。

2		Critical,High,Medium
このアドバイザのみ	Cisco ASA ソフトウェア	
あらゆるプラットフォーム		
Enter release number	Check	

Cisco Secure FTD デバイスのアップグレード手順については、該当の Cisco Secure FMC アップ

グレードガイドを参照してください。

関連情報

最適な Cisco Secure Firewall ASA、Cisco Secure FMC、Cisco Secure FTD の各ソフトウェアリリースの決定方法については、次の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco Secure Firewall ASA の互換性
Cisco Secure Firewall ASA アップグレードガイド
Cisco Secure Firewall Threat Defense 互換性ガイド

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のAda Greymiire氏とAlex Lumsden氏による社内セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-saml-LktTrwZP

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2026年3月4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。