Cisco IOx アプリケーション フレームワークの任意のファイル作成における脆弱性

High

アドバイザリーID : cisco-sa-caf-3dXM8exv CVE-2020-3238
初公開日 : 2020-06-03 16:00
バージョン 1.0 : Final
CVSSスコア : 8.1
回避策 : No workarounds available
Cisco バグ ID : CSCvr02052

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 IOx アプリケーション環境の Cisco アプリケーション フレームワーク コンポーネントの脆弱性により、認証されたリモートの攻撃者が、影響を受けるデバイスで実行されている仮想インスタンス内で任意のファイルの書き込みまたは変更を行う可能性があります。

この脆弱性は、ユーザ提供アプリケーションパッケージの入力の検証が不十分であることに起因します。Cisco IOx 内部で悪意のあるパッケージをアップロードできる攻撃者は、脆弱性をエクスプロイトして任意のファイルを変更する可能性があります。エクスプロイトが成功した場合の影響は、仮想インスタンスの範囲に限定され、Cisco IOx をホストしているデバイスには影響を及ぼしません。

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-caf-3dXM8exv

該当製品

脆弱性のある製品

この脆弱性は、リリース 1.9.0 より前の Cisco IOx アプリケーション フレームワーク リリースを実行している以下のシスコ製品に影響を及ぼします。

- 800 シリーズ産業用サービス統合型ルータ（産業用 ISR）
- 800 シリーズ サービス統合型ルータ（ISR）

- 1000 シリーズ Connected Grid ルータ（CGR1000）コンピューティング モジュール
- IC3000 産業用コンピューティング ゲートウェイ
- 産業用イーサネット（IE）4000 シリーズ スイッチ
- IOS XE ベースのデバイス：
  - 1000 シリーズ ISR
  - 4000 シリーズ ISR
  - ASR 1000 シリーズ アグリゲーション サービス ルータ
  - Catalyst 9x00 シリーズ スイッチ
  - Catalyst IE3400 高耐久性シリーズ スイッチ
  - エンベデッドサービス 3300 シリーズ スイッチ
- IR510 WPAN 産業用ルータ

修正済みのシスコ プラットフォーム リリースの詳細については、このアドバイザリの「修正済みソフトウェア」のセクションを参照してください。

デバイスステータスの評価

Cisco IOS XE ベースのデバイス

次の Cisco IOS XE ベースのデバイスの場合、管理者は特権 EXEC コマンド show iox-service を使用して、Cisco IOx アプリケーション フレームワークがデバイスで有効になっているかどうかを判断できます。

- 1000 シリーズ ISR
- 4000 シリーズ ISR
- ASR 1000 シリーズ アグリゲーション サービス ルータ
- Catalyst 9x00 シリーズ スイッチ
- Catalyst IE3400 高耐久性シリーズ スイッチ
- エンベデッドサービス 3300 シリーズ スイッチ

次の show iox-service コマンドの出力は、Cisco IOx アプリケーション フレームワークが有効になっているデバイスを示しています。

```
<#root>

switch#

show iox-service


.
.
.
IOx Infrastructure Summary:
---------------------------

IOx service (CAF)
```

```
    :
Running


IOx service (HA)     : Running
IOx service (IOxman) : Running
Libvirtd             : Running
Dockerd              : Running
```

IOx サービス（CAF）が実行状態になっている場合、フレームワークは有効になっています。

Cisco IE 4000 シリーズ スイッチ

管理者は、特権 EXEC コマンド show iox detail を使用して、デバイスで Cisco IOx アプリケーション フレームワークが有効になっているかどうかを判断できます。次の show iox detail コマンドの出力は、Cisco IOx アプリケーション フレームワークが有効になっているデバイスを示しています。

```
<#root>

switch#

 show iox detail


.
.
.
IOx Processes State:
--------------------

caf

                    :

Running


ioxhad                  : Running
libvirtd                : Running
monit                   : Running
```

caf が実行状態の場合、フレームワークは有効になっています。

Cisco IR510 WPAN 産業用ルータ

IOx（Linux）端末にアクセスできる管理者は、次の CLI コマンドを使用できます。

次のコマンドでは、IOx リリースを確認できます。

```
<#root>
```

```
#vi
/etc/platform/version
```

次のコマンドでは、Cisco IOx アプリケーション フレームワークのステータスを確認できます。

```
<#root>
#monit
summary
```

管理者は、制限付きアプリケーションプロトコル（CoAP）Simple Management Protocol（CSMP）GUI フィールドツール/デバイスマネージャ、または Field Network DIRECTOR（FND）から get TLV を使用して、IOx のステータスを確認することもできます。IOx ホストステータスを確認するための TLV の数値は 146 です。

```
<#root>
146
```

```
message IoxHostStatus {
required uint32 status =
1
;
optional string version = 2;
optional uint32 upTime = 3;
}
```

前述の TLV では、必要な uint32 ステータスの 1 は、ホストがアップ状態で動作していることを示しています。

次の TLV は、IOx ホストステータスを取得するために使用されます。

```
0 - unheard, 1 - up, 2 - down, 3 - stopped, 4 - disabled
version: Client firmware version
upTime: Client's uptime
```

Cisco CGR1000 コンピューティング モジュール

次の例に示すように、管理者は show iox host list detail | include IOX Server is running CLI コマンドを使用して、IOx 機能のステータスを確認できます。

<#root>

```
CGR1000#
show iox host list detail | include IOX Server is running


IOX Server is running.
  Process ID: 305
CGR1000#
```

Cisco IC3000 産業用コンピューティング ゲートウェイ

Cisco IC3000 産業用コンピューティング ゲートウェイでは、Cisco IOx 機能はデフォルトで有効になっています。次の例に示すように、管理者は show iox summary CLI コマンドを使用して、IOx 機能のステータスを確認できます。

<#root>

```
ic3k#
show iox summary

    IOx Infrastructure Summary:
    ---------------------------
    eid: IC3000-2C2F-K9+FOC2227Y304
    pfm: IC3000-2C2F-K9
    s/n: FOC2227Y304
    images: Lnx: 1.0.1., IOx: 1.7.0:r/1.7.0.0:fc6e9cf
    boot: 2018-09-17 17:37:55
    time: 2018-09-18 18:07:28
    load: 18:07:28 up 1 day, 29 min, 0 users, load average: 0.32, 0.11, 0.02
    memory: ok, used: 481/7854 (6%)
    disk: ok, used: /:270305/338869 (79%), /software:57272/87462892 (0%)
    process: warning, running: 4/5, failed: sshd
    networking: ok
    logs: ok, errors: caf (0)
    apps: ok,
```

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記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

回避策

この脆弱性に対処する回避策はありません。

Cisco IOx アプリケーション フレームワークを使用する必要がないお客様は、no iox 設定コマンドを使用してデバイス上で IOx を無効化することで、この脆弱性を軽減できます。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したが Cisco Service Contract をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

シスコは、Cisco IOx アプリケーション フレームワークのリリース 1.9.0 以降でこの脆弱性を修正しています。

次の表は、Cisco IOx アプリケーション フレームワークのリリース 1.9.0 以降をサポートする最初の修正済みソフトウェアリリースを示しています。

シスコ プラットフォーム	Cisco IOx アプリケーション フレームワークのリリース 1.9.0 以降のサポートが導入されているリリース
800 シリーズ産業用 ISR	Cisco IOS ソフトウェアリリース 15.9(3)M
800 シリーズの ISR	修正なし。Cisco 800シリーズISRのIOxはサポートが終了しています。
CGR1000 コンピューティング モジュール	CGR1000 リリース 1.10.0.6 用の IOx イメージ
IC3000 産業用コンピューティング ゲートウェイ	産業用コンピューティング ゲートウェイ ソフトウェア リリース 1.2.1
IE 4000 シリーズ スイッチ	Cisco IOS ソフトウェアリリース 15.2.(7a)E0b
IOS XE デバイス : • 1000 シリーズ ISR • 4000 シリーズ ISR • ASR 1000 シリーズ アグリゲーション サービス ルータ • Catalyst 9x00 シリーズ スイッチ • Catalyst IE3400 高耐久性シリーズ スイッチ • エンベデッドサービス 3300 シリーズ スイッチ	Cisco IOS XE ソフトウェアリリース 17.2(1)
IR510 WPAN 産業用ルータ	IR510 オペレーティング システム リリース 6.1.27

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-caf-3dXM8exv

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	2020 年 6 月 3 日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。