Cisco IOS XRソフトウェア圧縮ACLバイパスの脆弱性

アドバイザリーID : cisco-sa-comp3acl-vGmp6BQ3
初公開日 : 2023-09-13 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwe08950

CVE-2023-20190

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 IOS XRソフトウェアの従来のアクセスコントロールリスト(ACL)圧縮機能における脆弱性により、認証されていないリモートの攻撃者が、該当デバイスに設定されたACLによって提供される保護をバイパスできる可能性があります。

この脆弱性は、影響を受けるデバイスのインターフェイスに適用されるACLの圧縮モジュールにおける宛先アドレス範囲の符号化が正しく行われないことに起因します。攻撃者は、設定されたACLによって拒否されるべき該当デバイスを介してトラフィックを送信することにより、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で設定されているACL保護をバイパスし、デバイスが保護している可能性がある信頼できるネットワークにアクセス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。本脆弱性に対処する回避策がいくつかあります。

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-comp3acl-vGmp6BQ3

このアドバイザリは、2023年9月に公開されたCisco IOS XR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。これらのアドバイザリとそのリンクの一覧については、『Cisco Event Response: September 2023 Semiannual Cisco IOS XR 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

公開時点では、この脆弱性は、Cisco IOS XRソフトウェアの脆弱性が存在するリリースを実行していて、レベル2またはレベル3の圧縮が適用されたクラシックIPv4 ACLが適用されているシスコ製品に影響を与えました。オブジェクトグループを使用するハイブリッドACLは影響を受けません。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

デバイス設定の確認

IPv4 ACLにレベル2または3の圧縮が適用されているかどうかを確認するには、show running-config | include "compress level 2|compress level 3" CLIコマンドを使用します。コマンドの出力が返される場合、デバイスはこの脆弱性の影響を受けます。ただし、影響はACLの設定によって異なります。詳細については、「詳細」を参照してください。

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。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- IOS ソフトウェア
- IOS XE ソフトウェア
- NX-OS ソフトウェア

詳細

ハイブリッドACLはこの脆弱性の影響を受けません。クラシックACLは、次の両方の条件を満たす場合に、この脆弱性の影響を受けます。

- レベル2またはレベル3の圧縮レベル（ハードウェアプラットフォームによる）
- 同じ宛先アドレスでマスクが異なるアクセスコントロールエントリ(ACE)

従来のACLで内部でレベル2またはレベル3の圧縮を使用する場合、圧縮コードはACE内の重複するIPアドレスをチェックします。2つ以上のエントリが同じ宛先アドレスを共有している場合、次の例に示すように、最初のエントリからの宛先マスクが、それ以降の重複するすべてのエントリに適用されます。

例 1：

```
ipv4 access-list CSCwe08950
 10 deny icmp any 198.51.100.0 0.0.0.7 time-exceeded
 20 deny icmp any 198.51.100.0 0.0.0.3
 40 permit ipv4 any any
```

例1では、198.51.100.7へのICMPエコー要求はACE行40に到達し、許可される必要があります。ACE 20と10は同じ宛先アドレスを使用するため、圧縮が適用されると、最初の宛先マスクのみが圧縮されたACLに適用され、その結果ICMPエコー要求が拒否されます。

例 2：

```
ipv4 access-list CSCwe08950
 10 deny icmp any 198.51.100.0 0.0.0.7 time-exceeded
 20 permit ipv4 any 198.51.100.0 0.0.0.3
 30 permit ospf any any
```

例2では、ACLによってホスト198.51.100.3へのtelnetトラフィックが許可され、ホスト198.51.100.7へのtelnetトラフィックは許可されないものと想定しています。ただし、ACE 20はACE 10の重複する宛先アドレスであるため、ACL圧縮コードはACE 10マスクを使用し、許可されます。

例 3：

```
ipv4 access-list CSCwe08950
 10 deny icmp host 1.1.1.1 198.51.100.0 0.0.0.7 time-exceeded
 20 permit icmp host 1.1.1.1 198.51.100.0 0.0.0.255
 40 permit ipv4 host 1.1.1.1 198.51.100.0 0.0.0.15
 50 permit ospf any any
```

例3では、1.1.1.1から198.51.100.30へのICMPエコー応答が許可されると想定します。ただし、ACE 20はACE 10の重複する宛先アドレスであるため、圧縮はACE 10マスクを適用し、1.1.1.1から198.51.100.30へのICMPエコー応答は許可されません。1.1.1.1から198.51.100.15へのtelnetセッションも許可されているはずですが、ACE 40がACE 10の複製であるため、ACE 10マスクが使用され、削除されました。

回避策

この脆弱性に対処する回避策はありません。

重複する宛先アドレスに対してレベル2または3の圧縮を使用している場合は、従来のACLを確認し、それに応じて調整することをお勧めします。

この回避策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

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 セキュリティ アドバイザリ 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アップグレード ソリューション一式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。

修正済みリリース

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列はシスコソフトウェアリリースを示し、右の列はリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。

Cisco IOS XR リリース	First Fixed Release（修正された最初のリリース）
7.2 以前	修正済みリリースに移行。
7.3	7.3.5
7.4	修正済みリリースに移行。
7.5	7.5.4
7.6	修正済みリリースに移行。
7.7	修正済みリリースに移行。
7.8	7.8.2
7.9	7.9.1

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された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、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は確認しておりません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-comp3acl-vGmp6BQ3

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	2023-9-13

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。