SNMPメッセージ処理の脆弱性

アドバイザリーID : cisco-sa-20040420-snmp
初公開日 : 2004-04-20 21:00
バージョン 1.5 : Final
回避策 : No Workarounds available
Cisco バグ ID : CSCed68575

CVE-2004-0714

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 Internetwork Operating System(IOS)ソフトウェアリリーストレイン12.0S、12.1E、12.2、12.2S、12.3、12.3B、および12.3Tには、SNMP要求の処理に脆弱性が含まれている可能性があります。これが不正利用されると、デバイスのリロードが引き起こされる可能性があります。

この脆弱性は、Ciscoルータおよびスイッチの特定のIOSリリースにのみ存在します。この動作はコードの変更によって発生し、CSCed68575で解決されます。

この脆弱性はリモートでトリガーされる可能性があります。この脆弱性の不正利用に成功すると、デバイスのリロードが引き起こされる可能性があり、繰り返し不正利用されてサービス拒否(DoS)が発生する可能性があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-snmp で確認できます。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

この脆弱性は、CSCeb22276のコード変更によって発生しました。この変更は次のリリースにコミットされており、これらのリリースには脆弱性が存在します。

Cisco IOSソフトウェアが稼働しているCisco Catalyst ATMモジュールは該当しません。

ONS 15454および15454Eは、MLシリーズラインカードで設定されており、リリース4.60が稼働している場合に脆弱性が存在します。ONS 15454および15454Eソフトウェアには、MLシリ

ーズラインカードで稼働するCisco IOSソフトウェアの脆弱性のあるバージョンがバンドルされています。該当するリリースが稼働するMLシリーズラインカードが搭載されていない設定には、脆弱性は存在しません。リリース4.60には12.1(20)EOがバンドルされており、脆弱です。

CCOが公開している次のリリースには、SNMPの問題に対する脆弱性があることが確認されています。シスコの知る限り、その他の公開リリースは影響を受けません。ただし、更新が行われた場合、シスコはこのリストを変更できます。シスコが公開した暫定リリースまたはカスタムリリースにも脆弱性が存在する可能性があります。暫定ビルドの詳細については、http://www.cisco.com/warp/public/620/1.htmlのセクション3.6を参照してください。

Cisco IOSソフトウェアのアップグレードに関する完全な表については、このアドバイザリの「ソフトウェアバージョンと修正」セクションを参照してください。

- 12.0(23)S4
- 12.0(23)S5
- 12.0(24)S4
- 12.0(24)S4a
- 12.0(24)S5
- 12.0(26)S1
- 12.0(27)S
- 12.0(27)SV
- 12.0(27)SV1
- 12.1(20)E
- 12.1(20)E1
- 12.1(20)E2
- 12.1(20)EA1
- 12.1(20)EB
- 12.1(20)EC
- 12.1(20)EC1
- 12.1(20)EO
- 12.1(20)EU
- 12.1(20)EW
- 12.1(20)EW1
- 12.2(12g)
- 12.2(12h)M1
- 12.2(12h)
- 12.2(20)S
- 12.2(20)S1
- 12.2(20)SW
- 12.2(21)
- 12.2(21a)

- 12.2(21)SW
- 12.2(21)ZQ
- 12.2(23)
- 12.3(2)XC1
- 12.3(2)XC2
- 12.3(2)XE
- 12.3(2)XF
- 12.3(4)T
- 12.3(4)T1
- 12.3(4)T2
- 12.3(4)T2a
- 12.3(4)T3
- 12.3(4)XD
- 12.3(4)XD1
- 12.3(4)XG
- 12.3(5)
- 12.3(5a)B
- 12.3(5a)
- 12.3(5b)
- 12.3(6)

Cisco 製品で稼働しているソフトウェアを確認するには、デバイスにログインし、show version コマンドを発行してシステム バナーを表示します。Cisco IOSソフトウェアは、「Internetwork Operating System Software」または単に「IOS®」と表示されます。出力の次の行では、イメージ名がカッコで囲まれて表示され、その後に「Version」とIOSリリース名が続きます。その他の Cisco デバイスには show version コマンドがないか、異なる出力が返されます。

次の例は、IOSリリース12.0(3)が稼働し、インストールされているイメージ名がC2500-IS-Lであるシスコ製品を示しています。

```
Cisco Internetwork Operating System Software IOS (TM)

2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

リリーストレインラベルは「12.0」です。

次の例は、IOSリリース12.0(2a)T1を実行し、イメージ名がC2600-JS-MZの製品を示しています。

```
Cisco Internetwork Operating System Software IOS (tm)

C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Cisco IOSリリースの命名の詳細については、http://www.cisco.com/warp/public/620/1.html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

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

詳細

簡易ネットワーク管理プロトコル(SNMP)は、インターネットプロトコル(IP)ネットワーク内のデバイスのリモート管理および監視のための標準メカニズムを定義します。SNMPをサポートするデバイスまたはホストはSNMPエンティティです。SNMPエンティティには2つのクラスがあります。情報を要求し、要請されないメッセージを受信するSNMPマネージャと、要請に応答し、要請されないメッセージを送信するSNMPエージェントです。SNMPプロキシ機能をサポートするSNMPエンティティは、SNMPマネージャとSNMPエージェントの両方の機能を組み合わせています。

SNMP操作には2つのクラスがあります。「get」や「set」などの送信要求のある操作では、SNMPマネージャがSNMPエージェント上の管理オブジェクトの値を要求または変更します。「trap」や「inform」などの送信要求のない操作では、SNMPエージェントがSNMPマネージャに送信要求のない通知やアラームメッセージを提供します。「inform」操作は、基本的に確認応答された「トラップ」です。

すべてのSNMP操作は、ユーザデータグラムプロトコル(UDP)経由で転送されます。送信要求された操作は、SNMPマネージャによってエージェントのUDP宛先ポート161に送信されます。非送信請求の操作は、SNMPエージェントによってUDP宛先ポート162に送信されます。IOSでは、SNMPマネージャが「inform」操作に応答してSNMPエージェントに送信する確認応答は、SNMPプロセスの開始時に選択される、ランダムに選択された上位ポートに送信されます。

IOSにはSNMPエージェントとSNMPプロキシの両方の機能が実装されているため、IOSのSNMPプロセスは、初期化時にUDPポート161、162、およびランダムUDPポートでSNMP操作のリスニングを開始します。SNMPプロセスは、デバイスのブート時またはSNMPの設定時に開始されます。

次の一連の手順で高ポートを選択します。

1. 49152 ~ 59152の間の乱数が生成されます。
2. IOSは、そのUDPポートがすでに使用されているかどうかをチェックします。そうでない場合、そのUDPポートはSNMP「inform」確認応答メッセージを受信するように選択されます

。
3. ポートがすでに使用中の場合、IOSはポート番号を1ずつ増やして再度チェックし、開いているポートが見つかるまで増えます。

そのため、選択されたポートは59152より高い可能性がありますが、その可能性は低いと考えられます。

この脆弱性では、IOS SNMPプロセスが、UDPポート162およびランダムUDPポートでSNMP送信要求の処理を誤って試みています。これらのポートの1つで要求されたSNMP操作を処理しようとすると、デバイスでメモリ破損が発生し、リロードが発生する可能性があります。

脆弱性のあるポートに対するSNMPv1およびSNMPv2cの送信要求オペレーションでは、SNMPコミュニティストリングに対して認証チェックが実行され、攻撃の緩和に使用される場合があります。コミュニティストリングとコミュニティストリングACLを推測しにくくするベストプラクティスにより、この脆弱性はSNMPv1とSNMPv2cの両方で緩和される可能性があります。ただし、脆弱性のあるポートに対してSNMPv3要求の動作を行うと、デバイスがリセットされます。SNMPが設定されている場合、影響を受けるすべてのバージョンでSNMPバージョン1、2c、および3の動作が処理されます。

この脆弱性はDDTS CSCeb22276で導入され、DDTS CSCed68575で修正されています。

回避策

回避策の効果は、製品の組み合わせ、ネットワークトポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。該当する製品とリリースは多岐に渡るので、サービス プロバイダーやサポート機関に連絡し、ネットワーク内で使用するのに最も適した回避策を確認してから、実際に配備することを推奨いたします。

アンチスプーフィング方式によって、スプーフィングされたソース攻撃がネットワークに侵入するのを常に防止し、なおかつ、影響を受ける可能性のあるすべてのデバイスに次のアクセスリストを設定する場合は、次の回避策を長期的なソリューションとしてのみ検討する必要があります。

- 次のコマンドを発行すると、IOSが稼働するデバイスでSNMP処理を無効にできます。

```
no snmp-server
```

  コンフィギュレーションコマンドno snmp-server community <string> roを使用してパブリックコミュニティストリングを削除しても、SNMPサーバは稼働を続け、デバイスは脆弱であるため、十分ではありません。代わりにno snmp-serverコマンドを使用する必要があります。enableコマンドshow snmpを使用して、SNMPサーバのステータスを確認します。「%SNMP agent not enabled」という応答が表示されるはずです。

- アクセスコントロールリスト(ACL)を使用して、該当するポートへのトラフィックを拒否できます。ランダムな高いポートが49152 ~ 59152(最大65535)の範囲に収まることは保証できないため、次のアクセスリストの例では、49152 ~ 65535の範囲のすべてのUDPポートをブロックする方法を示しています。このセクションで後述する潜在的な副作用を理解するために注意する必要があります。
  Cisco IOSデバイスにはコミュニティストリング単位でSNMP要求の送信元アドレスをチェックするコミュニティストリングアクセスリストが設定されていますが、SNMPv3の脆弱性を緩和するには十分ではありません。
  rACLを使用するオプションがないプラットフォームでは、インターフェイスACLを使用して、信頼できるIPアドレスからルータへのUDPトラフィックを許可できます。
  注：SNMPはUDPに基づいているため、送信元のIPアドレスをスプーフィングして、信頼できるIPアドレスからこれらのポートへの通信を許可するACLを無効にできる可能性があります。
  次の拡張アクセスリストをネットワークに適用できます。次の例での前提事項は、ルータのインターフェイスに IP アドレス 192.168.10.1 および 172.16.1.1 が設定されていること、すべての SNMP アクセスが IP アドレス 10.1.1.1 の管理ステーションに限定されていること、およびその管理ステーションが IP アドレス192.168.10.1とだけ通信する必要があることです。

```
access-list 101 permit udp host 10.1.1.1 host 192.168.10.1 range 161 162
access-list 101 permit udp host 10.1.1.1 host 192.168.10.1 range 49152 65535
access-list 101 deny udp any host 192.168.10.1 range 161 162
access-list 101 deny udp any host 192.168.10.1 range 49152 65535
access-list 101 deny udp any host 172.16.1.1 range 161 162
access-list 101 deny udp any host 172.16.1.1 range 49152 65535
access-list 101 permit ip any any
```

  その後、次の設定コマンドを使用して、すべてのインターフェイスにaccess-listを適用する必要があります。

```
interface ethernet 0/0
ip access-group 101 in
```

  ルータがSNMPパケットを受け入れて処理するのを防ぐため、上記で指定した範囲のUDPトラフィックは、ルータの各IPアドレスに対して明示的にブロックする必要があることに注意してください。また、未知のホストからポート161へのトラフィックをブロックすることがベストプラクティスですが、この場合、ポート161は影響を受けず、不正利用を防ぐためにブロックする必要はありません。
  これらのUDPポートでルータと直接通信するすべてのデバイスは、上記のアクセスリストに具体的に記載する必要があります。Cisco IOSは、49152 ~ 65535の範囲のポートを、DNSクエリなどのアウトバウンドセッションの送信元ポートとして使用します。
  IP アドレスが多数設定されているデバイス、またはルータと通信する必要がある多数のホ

ストでは、この方法はスケーラブルなソリューションでない場合があります。
重要：Cisco IOSは、TFTP経由でアップグレードする際に同じ送信元ポート範囲を使用します。アップグレードプロセスにTFTPサーバからのダウンロードが含まれている場合は、ルータとTFTPサーバ間のUDPトラフィックを49152 ~ 65535の範囲で必ず許可してください。FTPなど、UDPに依存しない別のダウンロード方法も使用できます。
TFTP以外にも、影響を受ける可能性のある他のサービスには、ネットワークタイムプロトコル(NTP)、Remote Authentication Dial In User Service(RADIUS)、Domain Name Service(DNS)などがあります。この回避策の影響を最小限に抑えるには、IOSデバイスとサービスを提供するサーバ間のアクセスを明示的に許可します。上記の回避策を導入する前に、ネットワークへの影響を理解することが非常に重要です。

- 個々のポートのブロッキング
  IOSデバイスによって選択された大きいポート番号は、show ip socketsコマンドを使用して確認できます。その個々のポートへのUDPトラフィックは、ポート範囲全体ではなくブロックできます。ルータのリブート時またはSNMPサービスの停止後および再起動時に高ポートがランダムに選択されるため、このアプローチは理想的ではありません。ただし、これは、たとえばアップグレードの準備をしているときに脆弱性から自分自身を保護したいお客様にとって、短期的なソリューションになる可能性があります。

  show ip socketsコマンドの出力：

```
Router#sh ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
[snip]
 17   --listen--          192.168.10.72     161   0   0    1   0
 17   --listen--          192.168.10.72     162   0   0   11   0
 17   --listen--          192.168.10.72   49212   0   0   11   0
```

  上記の例は、3つのSNMP関連ポートがリッスンしていて、高いポートが49212にバインドされていることを示しています。
  49152 ~ 65535のポート範囲全体をブロックするのではなく、一時的な回避策として（ポート162に加えて）ポート49212をブロックできます。
- 受信ACL(rACL)
  分散プラットフォームの場合、rACLは、12000シリーズGSRのCisco IOSソフトウェアバージョン12.0(21)S2および7500シリーズの12.0(24)S以降のオプションである可能性があります。受信アクセス リストは、ルート プロセッサが有害なトラフィックの影響を受ける前に、そのトラフィックからデバイスを保護します。受信パスACLはネットワークセキュリティのベストプラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、優れたネットワークセキュリティへの長期的な付加機能として考慮する必要があります。CPU 負荷がライン カード プロセッサに分散されるため、メイン ルート プロセッサの負荷を軽減させるのに役立ちます。ホワイトペーパー『GSR: Receive Access Control Lists』では、デバイスへの正当なトラフィックを識別して許可し、望ましくないパケットをすべて拒否するのに役立ちます。

http://www.cisco.com/warp/public/707/racl.html

- インフラストラクチャ ACL（iACL）
  ネットワークを移動するトラフィックをブロックするのは往々にして困難ですが、インフラストラクチャ デバイスに送られてはならないトラフィックを識別し、ネットワークの境界でそのトラフィックをブロックすることは可能です。インフラストラクチャ ACL はネットワーク セキュリティのベスト プラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、優れたネットワーク セキュリティへの長期的な付加機能として考慮する必要があります。ホワイトペーパー『Protecting Your Core: Infrastructure Protection Access Control Lists』では、iACLのガイドラインと推奨される導入方法について説明しています。
  http://www.cisco.com/warp/public/707/iacl.html

修正済みソフトウェア

シスコは2004年4月20日に複数のアドバイザリをリリースしました。

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirtおよび後続のアドバイザリも参照して、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。

Cisco IOS ソフトウェアの表（下掲）の各行には、リリース トレインが記載されています。特定のリリーストレインに脆弱性が存在する場合、修正を含む最初のリリース（「最初の修正リリース」）とそれぞれの提供予定日が「リビルド」、「暫定」、および「メンテナンス」の各列に記載されます。特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。このようなリリースは、少なくとも、示されているリリース以上（最初の修正リリース ラベル以上）にアップグレードしてする必要があります。リリースを選択するときは、次の定義を念頭においてください。

- メンテナンス- 表の該当行のリリース群のうち、十分にテストされて安定しているため、強く推奨されるリリース。
- 再構築- 同じリリース群の以前のメンテナンス リリースまたはメジャー リリースから構築されたリリース。特定の障害に対する修正が含まれています。テストは十分ではありませんが、脆弱性を修正するために必要な最小限の変更だけが含まれています。
- 暫定- メンテナンス リリース間に定期的に構築されるリリース。厳密なテストは実施されていません。暫定は、脆弱性に対応しているリリースが他にない場合にだけ選択してください。暫定イメージは、次のメンテナンス リリースが利用可能になった後、すぐにアップグレードする必要があります。暫定リリースは製造部門を通じて入手することはできず、通常はCisco TACと事前に調整を行わないと、CCOからダウンロードできません。

特定のIOSリリースに関する情報を見つけるには、show versionコマンドによって報告されるリリース番号を、次の最初の列のメジャーリリースと比較します。たとえば、デバイスが12.3(5)を実行していると報告した場合は、テーブルで「12.3」の行を見つけます。右側のRebuild列に

12.3(5c)が表示されており、12.3(5) ~ 12.3(5b)に脆弱性があることが示されています。12.3(5c)はすでにCCOからダウンロードできるため、できるだけ早くアップグレードできます。

リリーストレインに「Vulnerable」というラベルが付いている場合は、別のリリーストレインへの移行を検討する必要があります。異なるリリーストレインのリリースラベルが下記の表に明記されている場合を除き、適切な移行パスを特定するためにCisco TACにサポートを依頼してください。移行が不可能な場合は、回避策が唯一の代替手段である可能性があります。

すべての場合において、アップグレードするデバイスに十分なメモリが実装されており、現在のハードウェアおよびソフトウェアの構成が新しいソフトウェア リリースでも適切にサポートされていることを確認する必要があります。情報が不明な場合は、Cisco TACに連絡して、下記の「修正済みソフトウェアの入手」セクションに示されているサポートを依頼してください。

Cisco IOS ソフトウェアのリリース名および省略形の詳細は、http://www.cisco.com/warp/public/620/1.html620 を参照してください。修正は、http://www.cisco.com/public/sw-center/ の Software Center から入手できます。

メジャー リリース	修正済みリリースの入手可能性		
該当する 12.0 ベースのリリース	リビルド	Interim	メンテナンス
12.0S	12.0(23)S6		
	12.0(24)S6		
	12.0(26)S2		
	12.0(27)S1		
12.0SV	12.0(27)SV2:TACにお問い合せくださ		

	い。ご要望に応じてご利用いただけます。		
該当する 12.1 ベースのリリース	リビルド	Interim	メンテナンス
12.1E	12.1(20)E3		
	12.1(22)E1		
12.1EA	12.1(20)EA1a		
12.1EB			12.1(22)EB
12.1EC	12.1(20)EC2:TACにお問い合せください。ご要望に応じてご利用いただけます。		
12.1EO	12.1(20)EO1		
12.1EU	12.1(20)EU1は2004年5月上旬にCCOに掲載		
12.1EW	12.1(20)EW2		
該当す	リビルド	Interim	メンテナンス

る 12.2 ベースのリリース			
12.2	12.2(12i)		
	12.2(21b)		
		12.2(23.6)：要求に応じて利用可能	12.2(24)
	12.2(23a)		
12.2S	12.2(20)S2		
			12.2(22)S
12.2SW			12.2(23)SW:2004年5月中旬に提供開始
該当する 12.3 ベースのリリース	リビルド	Interim	メンテナンス
12.3	12.3(5c)		
	12.3(6a)		
		12.3(7.7)：要	12.3(9):2004年6月

		求に応じて利用可能	中旬にCCOに登録予定。
12.3B	12.3(5)B1:2004年6月中旬にCCOに登録予定。		
12.3T	12.3(4)T4		
			12.3(7)T
12.3XC	脆弱性あり、2004年5月中旬にCCOにより12.3(8)Tに移行される		
12.3XD	12.3(4)XD2		
12.3XE	脆弱性あり、2004年5月中旬にCCOにより12.3(8)Tに移行される		
12.3XF	contact TAC		
12.3XG	12.3(4)XG1		
12.3XH			12.3(4)XH
12.3XK			12.3(4)XK
12.3XQ			12.3(4)XQ

オプティカル製品

製品	修正済みリリースの入手可能性
MLシリーズ回線を使用したCisco ONS 15454および15454E	4.62、2004年4月27日に入手可能

推奨事項

$propertyAndFields.get("recommendations")

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。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-snmp

改訂履歴

Revision 1.5	2004年5月5日	12.0S、12.1EB、12.2、12.2S、12.2SW、12.3、12.3T、12.3XH、12.3XK、および12.3XQのソフトウェアのアベイラビリティに関する情報を更新。新しいリリースは追加されていません。
リビジョン 1.4	2004年4月29日	「ソフトウェアバージョンと修正」セクションで、12.3XCのエントリを変更しました。
リビジョン 1.3	2004年4月23日	「該当製品」セクションで、各リリースを個別の行に記載しています。
リビジョ	2004年	「該当製品」セクションで、第4段

ン 1.2	4月23日	落を修正し、リリースのリストを更新。 「ソフトウェアバージョンと修正」セクションで、12.1EB、12.1EO、12.1EU、12.2SW、12.2ZQ、12.2XE、12.2XFのエントリを変更または追加
リビジョン 1.1	2004年4月22日	「ソフトウェアバージョンと修正」セクションで、オプティカル製品の表を追加し、IOSリリースの表を更新。 「該当製品」セクションに、Catalyst製品とオプティカル製品、および12.1(20)EOを追加。
リビジョン 1.0	2004年4月20日	初回公開リリース

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。