Cisco ONS 15216 OADM TelnetのDoS脆弱性

severity

アドバイザリーID : cisco-sa-20050713-ons

初公開日 : 2005-07-13 15:00

バージョン 1.0 : Final

回避策 : No Workarounds available

Cisco バグ ID :

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 ONS 15216 OADM(Optical Add/Drop Multiplexer)には、管理プレーンでサービス拒否状態を引き起こす可能性があるTelnetセッションの処理に関する脆弱性が存在します。Cisco ONS 15216 OADMを通過するトラフィック（中継トラフィック）は、管理プレーンがサービス拒否状態にある場合は影響を受けません。ただし、管理プレーンでサービス拒否状態をクリアするには、デバイスをリセットする必要があり、これは通過トラフィックに影響します。

シスコでは、この脆弱性に対処する無償ソフトウェアを提供しています。この脆弱性の影響を軽減するための回避策があります(「回避策」セクションを参照)。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050713-ons で公開されています。

該当製品

脆弱性のある製品

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のは、ソフトウェアリリース2.2.2以前を実行しているCisco ONS 15216 OADMだけです。

ソフトウェアリビジョンを確認するには、TL1セッションを起動し、TL1プロンプトで**RTRV-NE-GEN**コマンドを使用して、次の例のようにソフトウェアバージョン情報を取得します。

```
> RTRV-NE-GEN:<tid>::100;

TID-000 98-06-20 14-30-00 M001COMPLD"VENDOR=CISCO, MODEL=SOADM-1CH-1530.33,
SN=0001,SOFTWARE=2.0.0, SOFTWAREUPDATE=1-3-2001,FIRMWARE=1.2.7,
```

```
FIRMWAREUPDATE=1-3-2001,CHANNUM=1,LAMBDA1=1530.33,ALM-LOSDROP-WEST-1=ON,
ALM-LOSDROP-EAST-1=ON,NAME=SOADM-1,LONGITUDE=100,LATITUDE=45,
IPADDRESS=10.0.0.2,IPMASK=255.0.0.0,A_POWER=OPERATING, B_POWER=OPERATING";
```

この出力は、ONS 15216 OADMがソフトウェアリリース2.0.0を実行していることを示しています。

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

Telnetは、ネットワークデバイスのリモート管理に使用されるプロトコルです。これはRFC 854で定義されています。

Cisco ONS15216 OADMを使用すると、サービスプロバイダーは光伝送ネットワークから単一から複数の波長を追加および削除できます。

Cisco ONS 15216 OADMには、個別の管理プレーンとデータプレーンがあります。管理プレーンはデバイスの管理に使用され、通常はインターネットから分離されたネットワークに接続され、お客様の環境に対してローカルです。OADMによってスイッチングおよび送信されるトラフィックは、データプレーンを流れます。

Cisco ONS 15216 OADMを使用して特別に巧妙に細工されたデータストリームをTelnetセッションに送信すると、セッションがロックアップし、それ以上のTelnetセッションを確立できなくなります。Telnetセッションがロックアップされている間、データプレーンを流れるトラフィックは影響を受*けません*。この脆弱性を引き起こすには、TCPセッションが事前に確立されている必要があります。つまり、TCP 3ウェイハンドシェイクが発生している必要があります。これにより、攻撃中に送信元アドレスをスプーフィングすることが困難になります。

管理プレーンとの通信を復元するには、Cisco ONS 15216 OADMをリロードする必要があります。この操作は、データプレーンを流れるトラフィックに影響します。

この脆弱性は、Cisco Bug ID CSCee23360「Telnetセッションの終了後に通信が完全に失われる」に記載されています。

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。

Cisco ONGプラットフォームは、個別の管理プレーンとデータプレーンを提供します。確立されたネットワークのベストプラクティスでは、管理プレーンは、インターネットから完全に分離され、顧客のトラフィックからは到達不能なプライベートネットワークに接続することを推奨しています。

完全な管理とデータプレーンの分離が不可能な場合は、隣接ルータでAccess Control List（ACL；アクセスコントロールリスト）を使用して、特定のネットワーク管理ステーションおよびIPアドレス範囲からCisco ONS 15216 OADMへのTelnet接続だけを許可することをお勧めします。このタイプのフィルタリングは、ネットワークのベストプラクティスであるインフラストラクチャACLの一部として実装できます。iACLの詳細については、http://www.cisco.com/warp/public/707/iacl.htmlの「Protecting Your Core: Infrastructure Protection Access Control Lists」を参照してください。

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場合は、http://www.cisco.com/en/US/products/products_security_advisories_listing.htmlおよび後続のアドバイザリも参照して、問題の発生の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機器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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が明確でない場合は、Cisco Technical Assistance Center(TAC)に連絡して支援を求めてください。

このアドバイザリに記載されている脆弱性は、ONS 15216 OADMソフトウェアのリリース2.2.3以降で修正されています。脆弱性が確認されたソフトウェアを現在実行している場合は、次に説明するように、修正済みソフトウェアを入手する必要があります。

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。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050713-ons

改訂履歴

リビジョン 1.0	2005年7月13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。