Cisco ONS 15327、ONS 15454、ONS 15454 SDH、およびONS 15600における不正なパケットに関する脆弱性

アドバイザリーID : cisco-sa-20040721-ons
初公開日 : 2004-07-21 16:00
バージョン 1.0 : Final
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2004-1433
CVE-2004-1432
CVE-2004-1435
CVE-2004-1434

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

シスコは、Cisco ONS 15327 Edge Optical Transport Platform、Cisco ONS 15454 Optical Transport Platform、Cisco ONS 15454 SDH Multiplexer Platform、およびCisco ONS 15600 Multiservice Switching PlatformのTCP/IPスタックにおける複数の不正パケットの脆弱性を修正しました。

これらの脆弱性は、Cisco Bug ID

- CSCed06531(IP)
- CSCed86946(ICMP)
- CSCec88426/CSCec88508/CSCed85088/CSCeb07263/CSCec21429(TCP)
- CSCec59739/CSCed02439/CSCed22547（最後の確認応答）
- CSCec88402/CSCed31918/CSCed83309/CSCec85982/CSCec21435/CSCee03697(UDP)
- CSCea16455/CSCea37089/CSCea37185(SNMP)
- CSCee27329(passwd)

このアドバイザリの回避策セクションには、これらの脆弱性の影響を軽減する回避策があります。シスコは修正済みソフトウェアを提供しており、お客様にはこのソフトウェアへのアップグレードを推奨しています。

このアドバイザリは
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

20040721-ons に掲載されています。

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

脆弱性を含む製品は次のとおりです。

- CSCed06531(IP)

製品	該当するリリース
15327	4.6(0) および 4.6(1) 4.1(0) ~ 4.1(3) 4.0(0) ~ 4.0(2) 3.x(x)以前
15454、15454 SDH	4.6(0) および 4.6(1) 4.5(x) 4.1(0) ~ 4.1(3) 4.0(0) ~ 4.0(2) 3.x(x) 2.3(5) より前
15600	Not affected

- CSCed86946(ICMP)

製品	該当するリリース
15327	4.6(0) および 4.6(1) 4.1(0) ~ 4.1(3) 4.0(0) ~ 4.0(2) 3.x(x)以前
15454、15454 SDH	4.6(0) および 4.6(1) 4.5(x) 4.1(0) ~ 4.1(3) 4.0(0) ~ 4.0(2) 3.x(x) 2.3(5) より前
15600	Not affected

- CSCec88426/CSCec88508/CSCed85088/CSCeb07263/CSCec21429(TCP)

製品	該当するリリース
15327	4.6(0) および 4.6(1) 4.1(0) ~ 4.1(3) 4.0(0) ~ 4.0(2) 3.x(x)以前
15454、15454 SDH	4.6(0) および 4.6(1) 4.5(x) 4.1(0) ~ 4.1(3) 4.0(0) ~ 4.0(2) 3.x(x) 2.3(5) より前
15600	1.x(x)

- CSCec59739/CSCed02439/CSCed22547（最後の確認応答）

製品	該当するリリース
15327	4.6(0) および 4.6(1) 4.1(0) ~ 4.1(3) 4.0(0) ~ 4.0(2) 3.x(x)以前
15454、15454 SDH	4.6(0) および 4.6(1) 4.5(x) 4.1(0) ~ 4.1(3) 4.0(0) ~ 4.0(2) 3.x(x) 2.3(5) より前
15600	Not affected

- CSCec88402/CSCed31918/CSCed83309/CSCec85982/CSCec21435/CSCee03697(UDP)

製品	該当するリリース
15327	4.6(0) および 4.6(1) 4.1(0) ~ 4.1(3) 4.0(0) ~ 4.0(2) 3.x(x)以前
15454、15454 SDH	4.6(0) および 4.6(1) 4.5(x) 4.1(0) ~ 4.1(3)

	4.0(0) ~ 4.0(2) 3.x(x) 2.3(5) より前
15600	1.x(x)

- CSCea16455/CSCea37089/CSCea37185(SNMP)

製品	該当するリリース
15327	4.1(0) ~ 4.1(2) 4.0(0) ~ 4.0(2) 3.x(x)以前
15454、15454 SDH	4.5(x) 4.1(0) ~ 4.1(2) 4.0(0) ~ 4.0(2) 3.x(x) 2.3(5) より前
15600	Not affected

- CSCee27329(passwd)

製品	該当するリリース
15327	4.6(0) および 4.6(1)
15454、15454 SDH	4.6(0) および 4.6(1)
15600	Not affected

脆弱性を含んでいないことが確認された製品

説明のため、次の製品はこれらの脆弱性の影響を受けません。

- Cisco ONS 15800 シリーズ
- ONS 15500シリーズ拡張サービスプラットフォーム
- ONS 15302、ONS 15305、ONS 15200シリーズメトロDWDMシステム
- ONS 15190シリーズIPトランスポートコンセントレータ

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。

使用しているソフトウェアのリビジョンを確認するには、CTC管理ソフトウェアでHelp > Aboutウィンドウを表示します。

詳細

該当するCisco ONS 15327、ONS 15454、ONS 15454 SDH、およびONS 15600ハードウェアは、それぞれXTC、TCC/TCC+/TCC2、TCCi/TCC2、およびTSCコントロールカードによって管理されます。これらのコントロールカードは通常、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、顧客の環境に対してローカルです。これにより、インターネットからの脆弱性が悪用される可能性が制限されます。

- CSCed06531(IP)
  不正なIPパケットによって、XTC、TCC/TCC+/TCC2、およびTCCi/TCC2コントロールカードがリセットされる可能性があります。これらの不正なパケットが繰り返し送信されると、両方のコントロールカードが同時にリセットされる可能性があります。
  Cisco ONS 15600ハードウェアは、この問題の影響を受けません。
- CSCed86946(ICMP)
  不正なICMPパケットによって、XTC、TCC/TCC+/TCC2、およびTCCi/TCC2コントロールカードがリセットされる可能性があります。これらの不正なパケットが繰り返し送信されると、両方のコントロールカードが同時にリセットされる可能性があります。
  Cisco ONS 15600ハードウェアは、この問題の影響を受けません。
- CSCec88426/CSCec88508/CSCed85088/CSCeb07263/CSCec21429(TCP)
  不正なTCPパケットによって、XTC、TCC/TCC+/TCC2、TCCi/TCC2、およびTSCコントロールカードがリセットされる可能性があります。これらの不正なパケットが繰り返し送信されると、両方のコントロールカードが同時にリセットされる可能性があります。
  Cisco Bug ID CSCec88426、CSCec88508、およびCSCed85088に、Cisco ONS 15327、ONS 15454、およびONS 15454 SDHの問題が記載されています。また、Cisco Bug ID CSCeb07263およびCSCec21429に、Cisco ONS 15600ハードウェアの問題が記載されています。
  Cisco ONS 15600ハードウェアへのトラフィックの影響はなく、この問題が原因で影響を受けるのは管理機能だけです。
- CSCec59739/CSCed02439/CSCed22547（最後の確認応答）
  XTC、TCC/TCC+/TCC2、およびTCCi/TCC2コントロールカードは、オープンTCPポートに対するTCP-ACKサービス拒否(DoS)攻撃の影響を受けやすくなっています。このような攻撃を受けると、光デバイスのコントローラカードがリセットされます。
  TCP-ACK DoS攻撃は、3ウェイTCPハンドシェイクの完了に必要な通常の最終ACKを送信せず、無効な応答を送信して接続を無効なTCP状態に移行することによって実行されます。

  Cisco ONS 15600ハードウェアは、この問題の影響を受けません。
- CSCec88402/CSCed31918/CSCed83309/CSCec85982/CSCec21435/CSCee03697(UDP)
  不正なUDPパケットによって、XTC、TCC/TCC+/TCC2、TCCi/TCC2、およびTSCコントロールカードがリセットされる可能性があります。これらの不正なパケットが繰り返し送信されると、両方のコントロールカードが同時にリセットされる可能性があります。
  Cisco Bug ID CSCec88402、CSCed31918、CSCed83309、およびCSCec85982に、Cisco ONS 15327、ONS 15454、およびONS 15454 SDHでの問題が記載されています。また、Cisco Bug ID CSCec21435およびCSCee03697に、Cisco ONS 15600ハードウェアでの問題

が記載されています。
Cisco ONS 15600ハードウェアへのトラフィックの影響はなく、この問題が原因で影響を受けるのは管理機能だけです。

- CSCea16455/CSCea37089/CSCea37185(SNMP)
  不正なSNMPパケットによって、XTC、TCC/TCC+/TCC2、およびTCCi/TCC2コントロールカードがリセットされる可能性があります。これらの不正なパケットが繰り返し送信されると、両方のコントロールカードが同時にリセットされる可能性があります。
  Cisco ONS 15600ハードウェアは、この問題の影響を受けません。
- CSCee27329(passwd)
  アカウントに空白のパスワードが設定されていて、10文字を超えるパスワードでデバイスにログインしようとすると、ログイン試行は成功します。
  この脆弱性は、TL1ログインインターフェイスにのみ影響します。CTCログインインターフェイスには、この脆弱性の脆弱性はありません。
  CTCおよびTL1のユーザインターフェイスでは、パスワードとして空白のパスワードを設定できません。初期インストールプロセス中のCISCO15ユーザIDにのみ空白のパスワードがあり、初期インストールプロセスの一部として変更されます。
  Cisco ONS 15600ハードウェアは、この問題の影響を受けません。

『Internetworking Terms and Cisco Systems Acronyms』オンラインガイドは、http://www.cisco.com/univercd/cc/td/doc/cisintwk/から入手できます。

これらの脆弱性は、Bug IDとしてCisco Bug Toolkitに記載されています

CSCed06531(IP)、

CSCed86946(ICMP)、

CSCec88426/CSCec88508/CSCed85088/CSCeb07263/CSCec21429 (TCP)、

CSCec59739/CSCed02439/CSCed22547(Last-ACK)、

CSCec88402/CSCed31918/CSCed83309/CSCec85982/CSCec21435/CSCee03697 (UDP)、

CSCea16455/CSCea37089/CSCea37185(SNMP)、および

CSCee27329(passwd)(登録ユーザ専用)。

回避策

XTC、TCC/TCC+/TCC2、TCCi/TCC2、またはTSCコントロールカードを宛先とするTCP/IPトラフィックがネットワーク管理ワークステーションからのみ許可されるように、脆弱なネットワークデバイスの前に設置されたルータ/スイッチ/ファイアウォールにACL（アクセスコントロールリスト）を適用します。Ciscoルータでアクセスコントロールリスト(ACL)を適用する方法の例については、http://www.cisco.com/warp/public/707/tacl.htmlを参照してください。

これらの回避策を使用しても、ネットワーク管理ステーションの送信元IPアドレスに設定されているスプーフィングされたIPパケットがスイッチの管理インターフェイスに到達することは防止されないことに注意してください。アンチスプーフィングの詳細については、/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#sec_ipおよびhttp://www.ietf.org/rfc/rfc2827.txtを参照してください。Unicast Reverse Path Forwarding（ユニキャストRPF）機能は、ルータを通過する不正な、または偽造されたIP送信元アドレスによって引き起こされる問題を緩和するのに役立ちます。http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htmを参照してください。

CSCee27329(passwd)の脆弱性の場合は、ユーザデータベースに空のパスワードが設定されていないことを確認してください。CISCO15ユーザIDに強力なパスワードが設定されていることを確認します。

Cisco PSIRT では、該当ユーザが修正済みソフトウェア バージョンのコードにアップグレードすることを推奨しています。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

このセキュリティアドバイザリで参照されているすべての脆弱性に対する最初の修正済みソフトウェアリリースの表

製品	修正済みリリース
15327	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降
15454、15454 SDH	4.6(2) 以降 4.1(4) 以降

	4.0(3) 以降 2.3(5)
15600	5.0 以降

- CSCed06531(IP)

製品	修正済みリリース
15327	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降
15454、15454 SDH	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降 2.3(5)
15600	Not affected

- CSCed86946(ICMP)

製品	修正済みリリース
15327	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降
15454、15454 SDH	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降 2.3(5)
15600	Not affected

- CSCec88426/CSCec88508/CSCed85088/CSCeb07263/CSCec21429(TCP)

製品	修正済みリリース
15327	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降
15454、15454 SDH	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降

	2.3(5)
15600	5.0 以降

- CSCec59739/CSCed02439/CSCed22547（最後の確認応答）

製品	修正済みリリース
15327	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降
15454、15454 SDH	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降 2.3(5)
15600	Not affected

- CSCec88402/CSCed31918/CSCed83309/CSCec85982/CSCec21435/CSCee03697(UDP)

製品	修正済みリリース
15327	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降
15454、15454 SDH	4.6(2) 以降 4.1(4) 以降 4.0(3) 以降 2.3(5)
15600	5.0 以降

- CSCea16455/CSCea37089/CSCea37185(SNMP)

製品	修正済みリリース
15327	4.1(3) 以降 4.0(3) 以降
15454、15454 SDH	4.6(0) 以降 4.1(3) 以降 4.0(3) 以降 2.3(5)
15600	Not affected

- CSCee27329(passwd)

製品	修正済みリリース
15327	4.6(2) 以降
15454、15454 SDH	4.6(2) 以降
15600	Not affected

Cisco ONS 15600プラットフォームの脆弱性は、2004年9月に利用可能になるCisco ONSソフトウェアリリース5.0で修正されています。

アップグレード手順は次のとおりです。

Cisco ONS 15327ハードウェアを修正済みソフトウェアバージョンにアップグレードする手順については、http://www.cisco.com/univercd/cc/td/doc/product/ong/15327/327doc41/index.htmを参照してください。

Cisco ONS 15454ハードウェアを修正済みソフトウェアバージョンにアップグレードする手順については、http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r46docs/index.htmを参照してください。

Cisco ONS 15600ハードウェアを修正済みソフトウェアバージョンにアップグレードする手順については、http://cisco.com/univercd/cc/td/doc/product/ong/15600/index.htmを参照してください。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

これらの脆弱性は、お客様からシスコに報告された不正なICMPパケットの脆弱性を除き、シスコの社内ストレステストで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040721-ons

改訂履歴

リビジョン 1.0	2004年7月21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。