Cisco Catalyst 4500E Series Switch with Cisco Catalyst Supervisor Engine 7L-E Denial of Service Vulnerability

Advisory ID: cisco-sa-20120926-ecc

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-ecc

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。

Revision 1.0

For Public Release 2012 September 26 16:00 UTC (GMT)

内容

要約
該当製品
詳細
脆弱性スコア詳細
影響
ソフトウェア バージョンおよび修正
回避策
修正済みソフトウェアの入手
不正利用事例と公式発表
この通知のステータス：FINAL
情報配信
更新履歴
シスコ セキュリティ手順

要約

Supervisor Engine 7L-E を搭載した Catalyst 4500E シリーズは、巧妙に細工されたパケットを処理する際にサービス拒否（DoS）の脆弱性が存在します。結果として、デバイスの再起動が引き起こされる可能性があります。

シスコはこの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ました。

これらの脆弱性に対しては回避策がありません。

このアドバイザリは、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-ecc

注：2012 年 9 月 26 日の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開には 9 件の Cisco Security Advisory が含まれています。8 件のアドバイザリは Cisco IOS ソフトウェアの脆弱性に対処するもので、1 件は Cisco Unified Communications Manager の脆弱性に対処す

るものです。各 Cisco IOS ソフトウェア セキュリティ アドバイザリには、そのアドバイザリで詳述された脆弱性を解決する Cisco IOS ソフトウェア リリース、および 2012 年 9 月にバンドル公開したすべての Cisco IOS ソフトウェアの脆弱性を解決する Cisco IOS ソフトウェア リリースを記載しています。

個々の公開リンクは、次のリンクにある「Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication」内に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

該当製品

この脆弱性は、Cisco IOS XE ソフトウェア リリース 03.02.00.XO.15.0(2)XO を稼働する、Supervisor Engine 7L-E 搭載の Catalyst 4500E シリーズにのみ影響します。 デバイスの設定に関係なく、該当バージョンの Cisco IOS XE ソフトウェアを稼働しているデバイスには脆弱性が存在します。

ハードウェアのタイプを確認するには、デバイスにログインし、Cisco IOS XE ソフトウェア CLI コマンドの **show module** を発行します。次の例は、Catalyst Supervisor Engine 7L-E をインストールしている Catalyst 4500E シリーズを示しています。

```
switch#show module
Chassis Type : WS-C4507R+E

Power consumed by backplane : 40 Watts

Mod Ports Card Type                                Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 4     6  Sup 7L-E 10GE (SFP+), 1000BaseX (SFP)   WS-X45-SUP7L-E
CAT1532L4ZA
 5    48  10/100/1000BaseT (RJ45)                  WS-X4448-GB-
RJ45    JAB023456A3
```

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインし **show version** コマンドを実行してシステム バナーを表示させます。「Internetwork Operating System Software」、「Cisco IOS Software」あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。その後ろにイメージ名が括弧の間に表示され、続いてバージョンと Cisco IOS ソフトウェア リリース名が表示されます。他のシスコ デバイスでは、show version コマンドがない場合や、表示が異なる場合があります。

次の例は、Supervisor Engine 7L-E 搭載 Catalyst 4500E シリーズで Cisco IOS XE ソフトウェア リリース 03.02.00.XO.15.0(2)XO を稼働し、インストールされているイメージ名が cat4500e-universal.SPA であることを示しています。

```
Catalyst_4500#show version
Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch
Software (cat4500e-UNIVERSAL-M), Version 03.02.00.XO RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 22-Sep-11 19:53 by prod_rel_team


<---  --->
```

```
    System returned to ROM by reload
    System image file is "bootflash:/cat4500e-
    universal.SPA.03.02.00.XO.150-2.XO.bin"
    Last reload reason: Reload command


    License Information for 'WS-X45-SUP7L-E'
        License Level: lanbase   Type: Default. No valid license
    found.
        Next reboot license Level: lanbase


Catalyst_4500#show version
Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch Software
(cat4500e-UNIVERSAL-M), Version 03.02.00.XO RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 22-Sep-11 19:53 by prod_rel_team


<---  --->

System returned to ROM by reload
System image file is "bootflash:/cat4500e-universal.SPA.03.02.00.XO.150-
2.XO.bin"
Last reload reason: Reload command


License Information for 'WS-X45-SUP7L-E'
    License Level: lanbase   Type: Default. No valid license found.
    Next reboot license Level: lanbase
```

Cisco IOS ソフトウェア リリースの命名規則の追加情報は、以下のリンクのホワイト ペーパー「Cisco IOS and NX-OS Software Reference Guide」で確認できます。

脆弱性が存在する製品

次の製品は、Cisco IOS XE ソフトウェア リリース 03.02.00.XO.15.0(2)XO を稼働しているときに脆弱性の影響を受けます。

- Supervisor Engine 7L-E 搭載 Catalyst 4500E シリーズ スイッチ

脆弱性が存在しない製品

次の製品または機能はこの脆弱性の影響を受けません。

- Cisco Catalyst Supervisor Engine II
- Cisco Catalyst Supervisor Engine IV
- Cisco Catalyst Supervisor Engine V
- Cisco Catalyst Supervisor Engine 6-E および 6-LE
- Cisco Catalyst Supervisor Engine 7-E
- Cisco Catalyst 4500-X シリーズ スイッチ
- Cisco Catalyst 4900 シリーズ スイッチ
- Cisco ME 4924-10GE イーサネット アグリゲーション スイッチ

他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。

詳細

Supervisor Engine 7L-E を搭載した Cisco Catalyst 4500E シリーズには、サービス拒否

（DoS）の脆弱性が存在します。これにより、認証されていないリモートの攻撃者がデバイスのスーパーバイザ カードのリロードを発生させることができる可能性があります。

この脆弱性は、不正なネットワーク パケットの不適切な処理に起因します。認証されていないリモートの攻撃者は、該当デバイスに巧妙に細工されたパケットを送信するか、そのデバイスを経由して送信することで、脆弱性を不正利用できる可能性があります。不正利用が成功した場合、攻撃者は該当デバイスのスーパーバイザ カードをリロードさせることができ、DoS 状態が発生します。
巧妙に細工されたパケットを受信したデバイスは、uncorrected ECC に関するエラー メッセージを表示します。次の例は、このエラー メッセージを示しています。

%C4K_SWITCHINGENGINEMAN-4-VFEL2INTERRUPT: (Suppressed 9 times)VFE L2 sptMemory interrupt.valid: 1 addr: 0x0 data: 0x0 **uncorrected** ecc: 0
このようなパケットを 72 時間以内に 100 個受信すると、デバイスは再起動します。

同様のエラー メッセージを発行させるものの、結果的には corrected ECC エラー メッセージとなるパケットも存在します。このようなエラー メッセージは情報を通知するものであり、デバイス自体には影響はありません。次の例は、このエラー メッセージを示しています。

%C4K_SWITCHINGENGINEMAN-4-VFEL2INTERRUPT: VFE L2 sptMemory interrupt.valid: 1 addr: 0x0 data: 0x0 **corrected** ecc: 2

デバイスの設定に関係なく、Cisco IOS XE ソフトウェア リリース 03.02.00.XO.15.0(2)XO を稼働しているデバイスには脆弱性が存在します。

この脆弱性は、Cisco Bug ID CSCty88456（ 登録ユーザのみ ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2012-4622 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCty88456 - Catalyst 4500E series switch with Supervisor Engine 7L-E Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

不正利用が成功した場合、該当デバイスでスーパーバイザ カードがリロードされる可能性があります。繰り返し悪用されると、持続的な DoS 攻撃につながります。

ソフトウェア バージョンおよび修正

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/ の Cisco Security Advisories and Responses アーカイブや、本アドバイザリ以降に公開のアドバイザリを参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

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。情報が不明確な場合は、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。

Cisco IOS ソフトウェア

Cisco IOS ソフトウェアは、このアドバイザリで説明されている脆弱性の影響は受けません。

Cisco IOS XE ソフトウェア

この脆弱性は、Cisco IOS XE ソフトウェア リリース 03.02.00.XO.15.0(2)XO にのみ影響します。

該当の Cisco IOS XE ソフトウェア リリースを稼働しているデバイスは、リリース 3.3.0.SG 以降に移行する必要があります。

Cisco	First Fixed	First Fixed Release for All

IOS XE Software Release	Release	Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication
2.1.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.2.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.3.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.4.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.5.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
2.6.x	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.1.xS	Not vulnerable	3.1.4S
3.1.xSG	Not vulnerable	Vulnerable; migrate to 3.2.5SG or later.
3.2.xS	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.2.xSG	Not vulnerable	3.2.5SG
3.2.xXO	Vulnerable; migrate to 3.3.0SG or later.	Vulnerable; migrate to 3.3.1SG or later.
3.3.xS	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.3.x.SG	Not vulnerable	3.3.1SG
3.4.xS	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.5.xS	Not vulnerable	Vulnerable; migrate to 3.6.0S or later.
3.6.xS	Not vulnerable	Not vulnerable
3.7.xS	Not vulnerable	Not vulnerable

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、『Cisco IOS XE 2 Release Notes』、『Cisco IOS XE 3S Release Notes』、『Cisco IOS XE 3SG Release Notes』を参照してください。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、このアドバイザリで説明されている脆弱性の影響は受けません。

回避策

この脆弱性に対する回避策はありません。Port Access Control List（PACL）と VLAN Access Control List（VACL）を使用してもこの脆弱性は回避されません。

修正済みソフトウェアの入手

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 アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

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、ご購入いただいたフィーチャ 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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレードを入手することができます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、適切な処置について支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策または修正が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

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シスコのサービス契約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購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC を通して無償アップグレードをお求めください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（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とその公表は確認しておりません。

この脆弱性は、お客様のサービス リクエストの処理中に発見されました。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-ecc

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

このアドバイザリに関する今後の更新があれば、Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2012-September-26	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。