

## 複数の Cisco Systems 製品におけるセキュリティ上の弱点(脆弱性)の注意喚起

IPA(独立行政法人情報処理推進機構、理事長:西垣 浩司)は、複数の Cisco Systems 製品におけるセキュリティ上の弱点(脆弱性)に関する注意喚起を、2009年5月29日に公表しました。

URL: [http://www.ipa.go.jp/security/vuln/documents/2009/200905\\_cisco.html](http://www.ipa.go.jp/security/vuln/documents/2009/200905_cisco.html)

この脆弱性は、外部から攻撃を受けた場合に、重要なファイルへアクセスされるというものです。

悪用されると、コンピュータ上の重要なファイルを盗まれたり、改ざんされたり、コンピュータが悪意あるユーザによって制御される可能性があります。

対策方法は「ベンダが提供する対策済みバージョンに更新する、もしくは『CiscoWorks Common Services』の TFTP サービスを停止する」ことです。

### 1. 概要

シスコシステムズ社(Cisco Systems, Inc.)が提供する「Cisco Security Manager」などの複数のソフトウェア製品には、ネットワーク管理をするための機能「CiscoWorks Common Services」が組み込まれています。

「CiscoWorks Common Services」には、ネットワークを通じてファイルを転送する仕組み(TFTP<sup>1</sup>サービス)に問題があり、ディレクトリ・トラバーサルというセキュリティ上の弱点(脆弱性)が存在します。この弱点が悪用されると、外部から攻撃を受けた場合に、コンピュータ上の任意のファイルへ外部からアクセスされてしまう可能性があります。

詳細は、下記の URL を参照してください。

<http://www.cisco.com/warp/public/707/cisco-sa-20090520-cw.shtml>

最新情報は、下記の URL を参照してください。

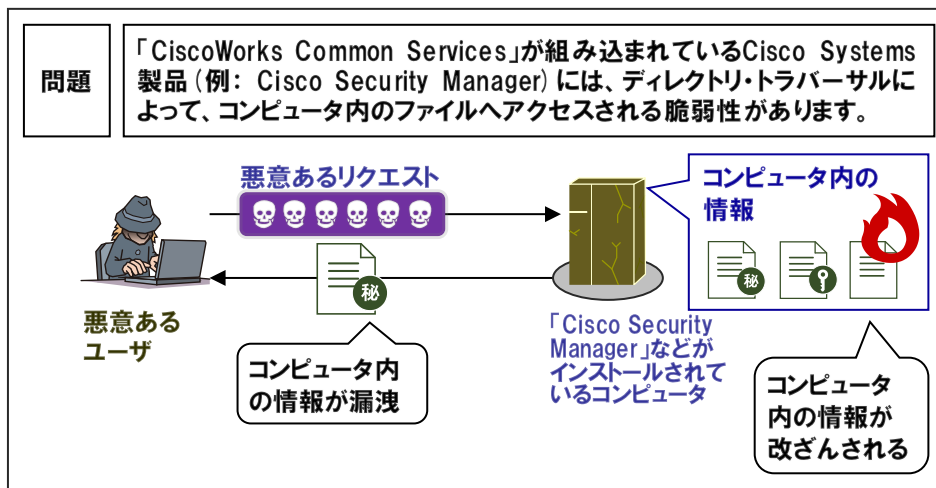
<http://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-000032.html>

本脆弱性情報は、情報セキュリティ早期警戒パートナーシップに基づき、2008年10月28日に以下の報告者からIPAに届出があり、JPCERT/CC(有限責任中間法人 JPCERT コーディネーションセンター)が製品開発者と調整を行ない、2009年5月29日に公表したものです。

報告者: エヌ・ティ・ティ・データ・セキュリティ株式会社 岡田 潤 氏

### 2. 脆弱性による影響

外部から攻撃されると、コンピュータ上のファイルへアクセスされる可能性があります。ファイルへアクセスされることで、コンピュータ内の重要な情報を盗まれたり、改ざんされたり、コンピュータが悪意あるユーザによって制御される可能性があります。



### 3. 対策方法

対策方法は「ベンダが提供する対策済みバージョンに更新する、もしくは『CiscoWorks Common Services』の TFTP サービスを停止する」ことです。

### 4. 本脆弱性の深刻度<sup>2</sup>

#### (1) 評価結果

本脆弱性の深刻度 (CVSS <sup>3</sup> 基本値の範囲)	<input type="checkbox"/> レベル I(注意) (0.0~3.9)	<input type="checkbox"/> レベル II(警告) (4.0~6.9)	<input checked="" type="checkbox"/> レベル III(危険) (7.0~10.0)
本脆弱性の CVSS 基本値			10.0

#### (2) CVSS 基本値の評価内容

AV: 攻撃元区分	<input type="checkbox"/> ローカル	<input type="checkbox"/> 隣接	<input checked="" type="checkbox"/> ネットワーク
AC: 攻撃条件の複雑さ	<input type="checkbox"/> 高	<input type="checkbox"/> 中	<input checked="" type="checkbox"/> 低
Au: 攻撃前の認証要否	<input type="checkbox"/> 複数	<input type="checkbox"/> 単一	<input checked="" type="checkbox"/> 不要
C: 機密性への影響	<input type="checkbox"/> なし	<input type="checkbox"/> 部分的	<input checked="" type="checkbox"/> 全面的
I: 完全性への影響	<input type="checkbox"/> なし	<input type="checkbox"/> 部分的	<input checked="" type="checkbox"/> 全面的
A: 可用性への影響	<input type="checkbox"/> なし	<input type="checkbox"/> 部分的	<input checked="" type="checkbox"/> 全面的

■: 選択した評価結果

AV: Access Vector, AC: Access Complexity, Au: Authentication, C: Confidentiality Impact, I: Integrity Impact, A: Availability Impact

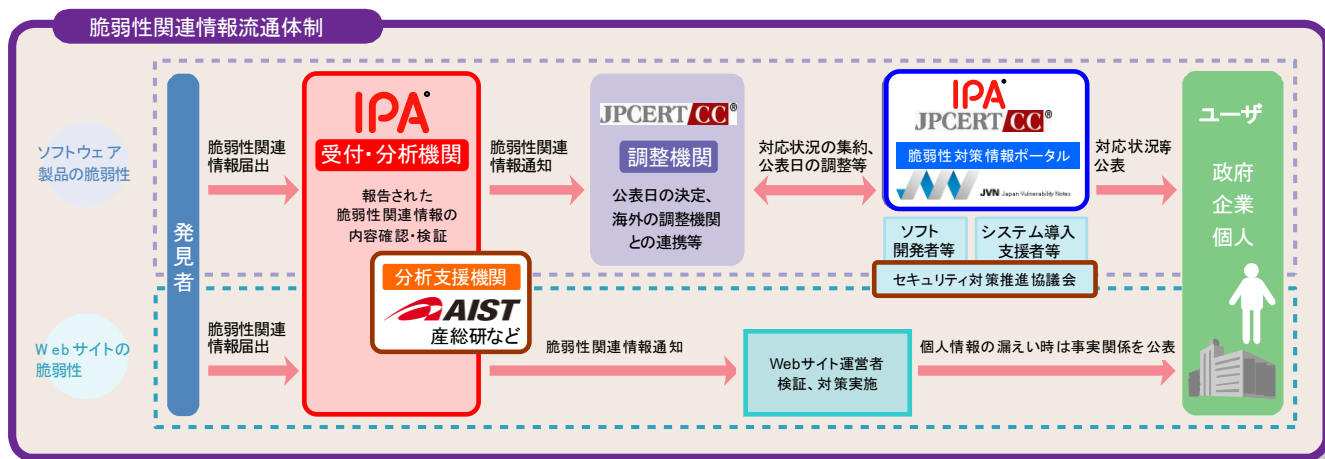
### 5. 本脆弱性の CWE<sup>4</sup>分類

本脆弱性の CWE 分類は、「パス・トラバーサル(CWE-22)」です。

### 6. 参考情報

#### (1) 「情報セキュリティ早期警戒パートナーシップ」について

ソフトウェア製品及びウェブサイトの脆弱性対策を促進し、コンピュータウイルスやコンピュータ不正アクセス等によって、不特定多数のコンピュータ(パソコン)に対して引き起こされる被害を予防するため、経済産業省の告示に基づき、官民の連携体制「情報セキュリティ早期警戒パートナーシップ」を整備し運用しています。



※JPCERT/CC: 有限責任中間法人 JPCERT コーディネーションセンター、産総研: 独立行政法人 産業技術総合研究所

<sup>1</sup> Trivial File Transfer Protocol。ネットワークを通じてコンピュータ間でファイルを転送するための仕組み。

<sup>2</sup> 脆弱性の深刻度評価の新バージョン CVSS v2 への移行について。http://www.ipa.go.jp/security/vuln/SeverityLevel2.html

<sup>3</sup> Common Vulnerability Scoring System。共通脆弱性評価システム。http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html

<sup>4</sup> Common Weakness Enumeration。共通脆弱性タイプ一覧。http://www.ipa.go.jp/security/vuln/CWE.html

■ 本件に関するお問い合わせ先  
IPA セキュリティセンター 山岸/渡辺  
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: [vuln-inq@ipa.go.jp](mailto:vuln-inq@ipa.go.jp)

■ 報道関係からのお問い合わせ先  
IPA 戦略企画部広報グループ 横山/大海  
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: [pr-inq@ipa.go.jp](mailto:pr-inq@ipa.go.jp)