

複数の Cisco 製スイッチの脆弱性対策について

IPA(独立行政法人情報処理推進機構、理事長:藤江 一正)は、複数の Cisco 製スイッチにおける脆弱性に関する注意喚起を、2013年3月7日に公表しました。対策方法は「**最新版へアップデートする**」ことです。

1. 概要

シスコシステムズ合同会社が提供する Cisco Small Business シリーズのスイッチには、サービス運用妨害 (DoS) 状態となる脆弱性が存在します。この脆弱性が悪用されると、該当する製品が一時的に使用不能となる可能性があります。

下記のサイトから、影響を受けるソフトウェアおよび修正済みバージョンの情報を入手して、更新してください。

<http://tools.cisco.com/security/center/viewAlert.x?alertId=27502>

最新情報は、次の URL を参照下さい。

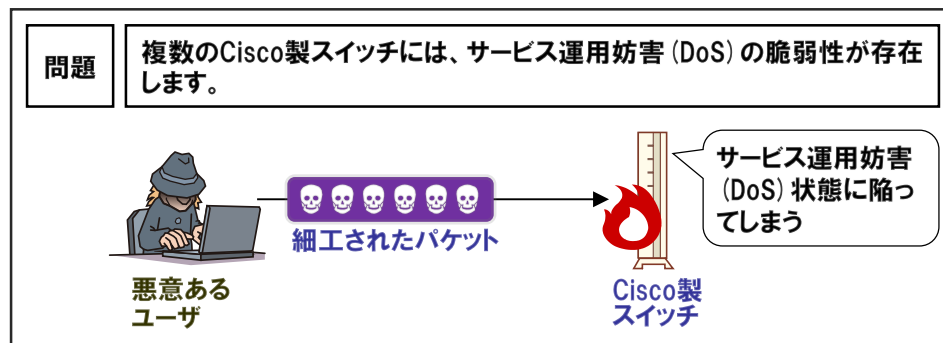
<http://jvndb.jvn.jp/jvndb/JVNDB-2013-000017>

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、以下の報告者から IPA が届出を受け、JPCERT/CC(一般社団法人 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、2013年3月7日に公表したものです。

報告者: 株式会社富士通研究所 児島 尚 氏、中田 正弘 氏(2012年4月6日届出)

2. 脆弱性による影響

遠隔の第三者によって、サービス運用妨害(DoS)攻撃を受ける可能性があります。



3. 対策方法

対策方法は「開発者が提供する情報をもとに、最新版へアップデートする」ことです。

4. 本脆弱性の深刻度^{(*)1}

(1) 評価結果

本脆弱性の深刻度 (CVSS ^{(*)2} 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			7.8

(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	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 checked="" type="checkbox"/> なし	<input type="checkbox"/> 部分的	<input type="checkbox"/> 全面的
I: 完全性への影響	<input checked="" type="checkbox"/> なし	<input type="checkbox"/> 部分的	<input 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

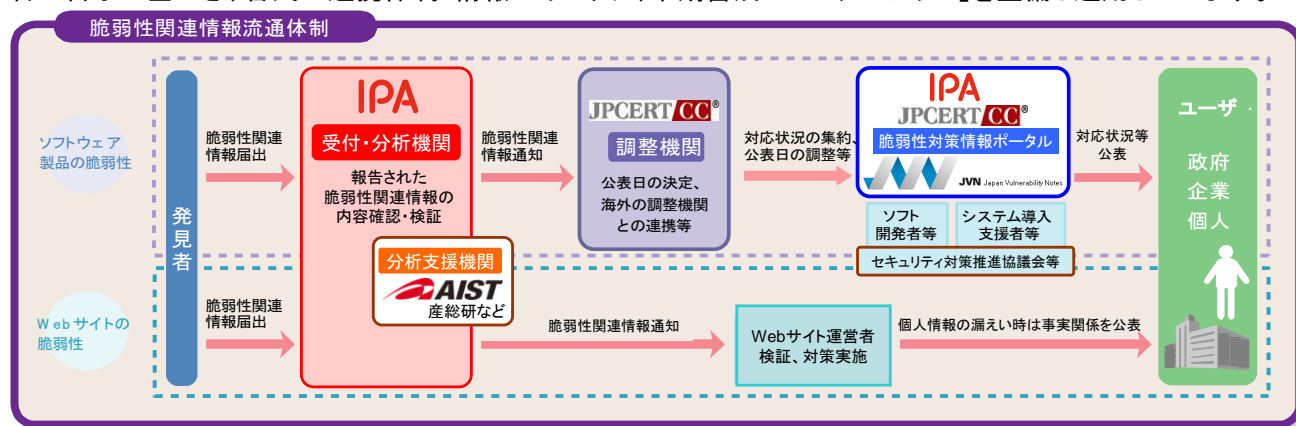
5. 本脆弱性の CWE^{(*)3} 分類

本脆弱性の CWE 分類は、「情報不足 (CWE-noinfo)」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

ソフトウェア製品およびウェブサイトの脆弱性対策を促進し、コンピューターウイルスやコンピューター不正アクセス等によって、不特定多数のコンピューター(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。



※IPA: 独立行政法人 情報処理推進機構、JPCERT/CC: 一般社団法人 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

■ 本件に関するお問い合わせ先
 IPA 技術本部 セキュリティセンター 中野/谷口
 Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: 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/佐々木
 Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

(*)1 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>
 (*)2 Common Vulnerability Scoring System. 共通脆弱性評価システム。 <http://www.ipa.go.jp/security/vuln/CVSS.html>
 (*)3 Common Weakness Enumeration. 共通脆弱性タイプ一覧。 <http://www.ipa.go.jp/security/vuln/CWE.html>