

## 「CapsSuite Small Edition PatchMeister」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、「CapsSuite Small Edition PatchMeister」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、2010年5月17日に公表しました。

URL: [http://www.ipa.go.jp/about/press/20100517\\_2.html](http://www.ipa.go.jp/about/press/20100517_2.html)

これは、「クライアントサービス for PTM」をインストールしているサーバもしくは端末が外部から攻撃を受けた場合に、OSのシャットダウン、または再起動をされるというものです。

対策方法は「開発者が提供する対策済みバージョンに更新する」ことです。

### 1. 概要

日本電気株式会社が開発している「CapsSuite Small Edition PatchMeister」はセキュリティパッチの適用管理を行うための製品です。

この「CapsSuite Small Edition PatchMeister」の「クライアントサービス for PTM」には、サービス運用妨害(DoS)状態となる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、「クライアントサービス for PTM」をインストールしているサーバもしくは端末のOSをシャットダウン、または再起動されてしまう可能性があります。

詳細は、次のURLを参照して下さい。

<http://www.nec.co.jp/security-info/secinfo/nv10-005.html>

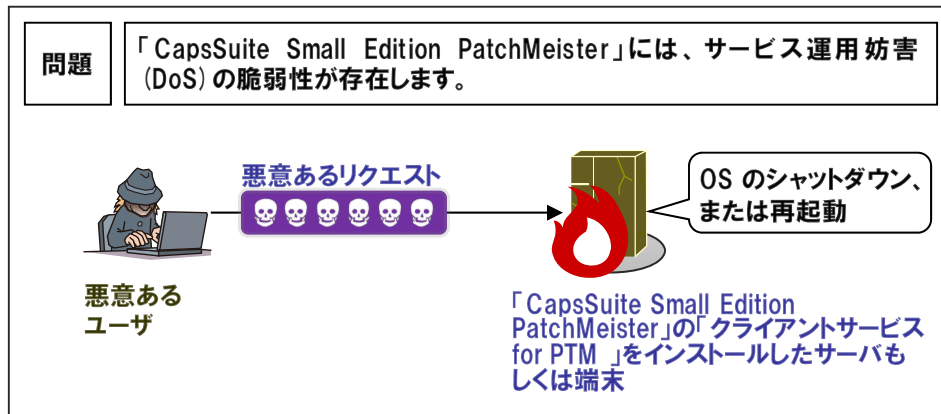
最新情報は、次のURLを参照下さい。

<http://jvndb.jvn.jp/jvndb/JVNDB-2010-000020>

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、2010年4月23日にIPAおよびJPCERT/CCが製品開発者自身から脆弱性および対策情報の連絡を受け、本日公表したものです。

### 2. 脆弱性による影響

遠隔の第三者により、「クライアントサービス for PTM」をインストールしているサーバもしくは端末において、OSのシャットダウン、または再起動を行われる可能性があります。



### 3. 対策方法

対策方法は「開発者が提供する対策済みバージョンに更新する」ことです。

### 4. 本脆弱性の深刻度<sup>1</sup>

#### (1) 評価結果

本脆弱性の深刻度 (CVSS <sup>2</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			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	<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 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

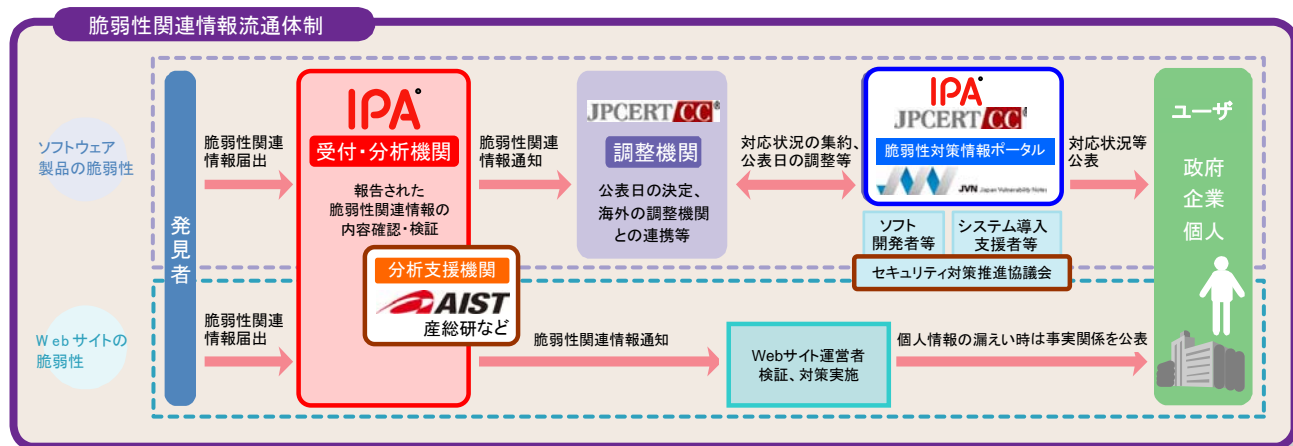
### 5. 本脆弱性の CWE<sup>3</sup>分類

本脆弱性の CWE 分類は、「設計上の問題 (CWE-DesignError)」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: 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 セキュリティセンター 渡辺/大森  
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)

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