

## 「SEIL シリーズ」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:藤江 一正)は、「SEIL シリーズ」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、2011年2月28日に公表しました。「SEIL シリーズ」上で任意のコードを実行される可能性があります。対策方法は「開発者が提供する修正済みファームウェアに更新する」ことです。

### 1. 概要

「SEIL シリーズ」は、株式会社インターネットイニシアティブが提供するルータ製品です。

「SEIL シリーズ」には、インターネット接続等で使用される PPPoE パケットの処理に問題があるため、バッファオーバーフロー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、「SEIL シリーズ」上で任意のコードを実行される可能性があります。

下記のサイトから修正済みバージョンを入手して、更新してください。

<http://www.seil.jp/support/security/a01001.html>

最新情報は、次の URL を参照下さい。

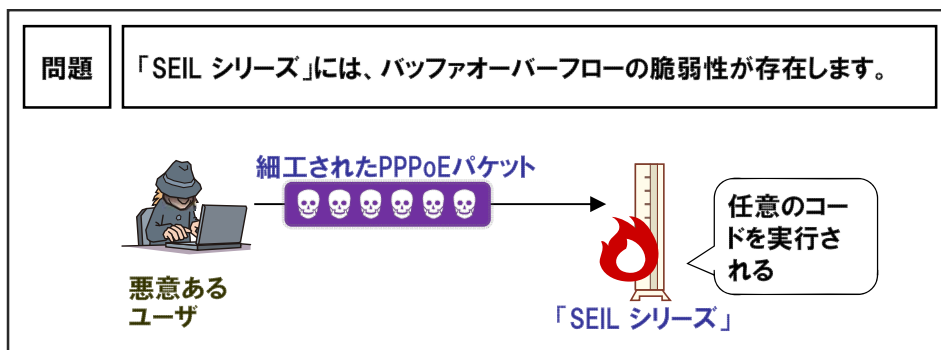
<http://jvndb.jvn.jp/jvndb/JVNDB-2011-000014>

本脆弱性情報は、2011年2月18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

「SEIL シリーズ」上で任意のコードを実行される可能性があります。

なお、開発者によると SEIL/x86 全バージョン、および SEIL/B1、SEIL/X1、SEIL/X2 の 3.00 から 3.11 まででは、本脆弱性の影響は PPP アクセスコンセントレータ(PPPAC)機能の停止などに限られるとのことです。



### 3. 対策方法

対策方法は「開発者が提供する修正済みファームウェアの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			8.3

#### (2) CVSS 基本値の評価内容

AV: 攻撃元区分	<input type="checkbox"/> ローカル	<input checked="" type="checkbox"/> 隣接	<input 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

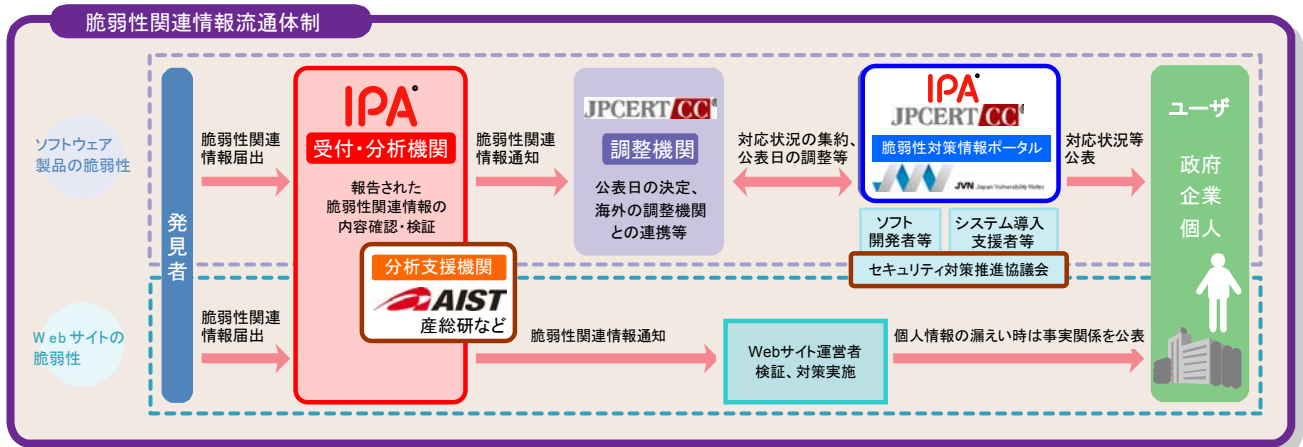
### 5. 本脆弱性の CWE<sup>3</sup>分類

本脆弱性の CWE 分類は、「バッファエラー (CWE-119)」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>