

「一太郎シリーズ」における3つのセキュリティ上の弱点(脆弱性)の注意喚起

独立行政法人 情報処理推進機構(略称:IPA、理事長:藤原武平太)は、「一太郎シリーズ」における3つのセキュリティ上の弱点(脆弱性)に関する注意喚起を、本日公表しました。

(URL: http://www.ipa.go.jp/security/vuln/200710_1chitaro.html)

これは、「一太郎シリーズ」の利用者が、ウェブブラウザやメール経由で悪意ある文書ファイルを開覧した場合に、任意のコードが実行されてしまうというものです。

悪用されると、システムが破壊されたり、ウイルスやボットに感染させられたりしてしまう可能性があります。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」ことです。

1. 概要

「一太郎シリーズ」は、日本語ワープロソフトです。「一太郎シリーズ」は、文章を作成するソフトウェアの一つとして、日本国内で広く利用されています。

「一太郎シリーズ」には、文書ファイルを読みこむ際に、3つのバッファオーバーフロー¹というセキュリティ上の弱点(脆弱性)があるため、任意のコードが実行されてしまう可能性があります。

脆弱性による影響が大きいことと、「一太郎シリーズ」の普及状況より、この影響を受ける利用者が国内に広く存在すると判断し、注意喚起を行いました。

最新情報は、次のURLを参照して下さい。

http://www.ipa.go.jp/security/vuln/documents/2007/JVN_50495547.html

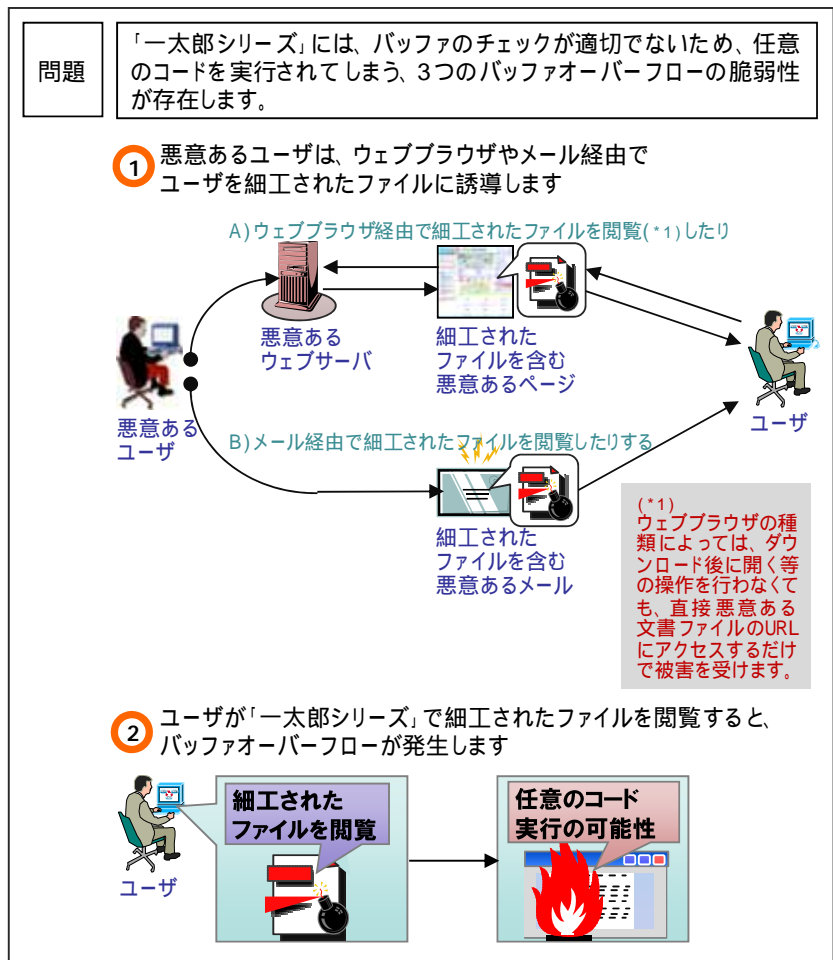
2. セキュリティ上の弱点(脆弱性)による影響

「一太郎シリーズ」の利用者が、ウェブブラウザで悪意ある文書ファイルを開覧したり、メール経由で悪意ある文書ファイルを開覧した場合に、システムが破壊されたり、ウイルスやボットに感染させられたりしてしまう可能性があります。

特に、ウェブブラウザでの閲覧の場合、ウェブブラウザの種類によっては、ダウンロード後に開く等の操作を行わなくても、悪意あるURLにアクセスするだけで被害を受けてしまう可能性があります。

(2007/10/26 追記)

結果として、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」ことです。

4. 本脆弱性の深刻度²

(1) 評価結果

本脆弱性の深刻度 (CVSS ³ 基本値の範囲)	レベルⅠ(注意) (0.0～3.9)	レベルⅡ(警告) (4.0～6.9)	レベルⅢ(危険) (7.0～10.0)
本脆弱性の CVSS 基本値		6.8	

(2) CVSS 基本値の評価内容

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

: 選択した評価結果

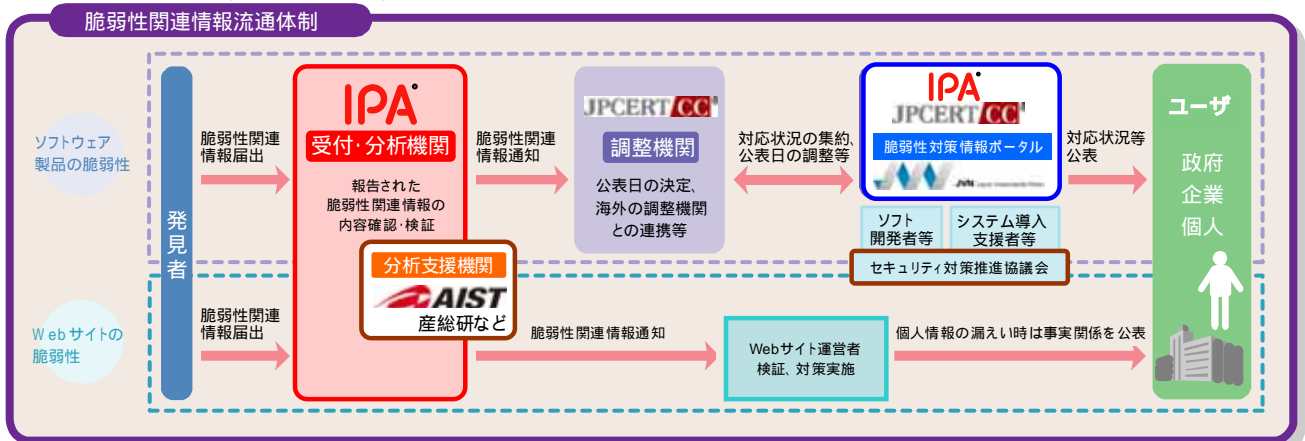
AV: Access Vector, AC: Access Complexity, Au: Authentication, C: Confidentiality Impact, I: Integrity Impact, A: Availability Impact

5. 参考情報

「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。

なお、今回公表した脆弱性情報は、2007年8月9日にIPAが届出を受け、有限責任中間法人 JPCERT コーディネーションセンター (JPCERT/CC) が、製品開発者と調整を行ない、本日公表したものです。



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

本内容に関するお問い合わせ先
 独立行政法人 情報処理推進機構 セキュリティセンター(IPA/ISEC)
 Tel:03-5978-7527 Fax:03-5978-7518 E-mail: vuln-inq@ipa.go.jp

報道関係からの問い合わせ先
 独立行政法人 情報処理推進機構 戦略企画部 広報グループ 横山/佐々木
 Tel03-5978-7503 FAX03-5978-7510 E-mail: pr-inq@ipa.go.jp

更新履歴

- 2007年10月25日 掲載
- 2007年10月26日 被害を受ける条件を明確化しました。

¹ バッファオーバーフローの概要や想定される脅威、対策などは、「セキュア・プログラミング講座」を参照下さい。
<http://www.ipa.go.jp/security/awareness/vendor/programmingv2/cc10.html>

² 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>

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