

「SugarCRM」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、「SugarCRM」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8月24日に公表しました。

URL: http://www.ipa.go.jp/security/vuln/documents/2009/200908_sugarcrm.html

この脆弱性は、「SugarCRM」にログインした攻撃者により任意の SQL 文が実行されるというものです。悪用されると、「SugarCRM」上に登録されている個人情報が入り、データが削除されたりするなど、データベースを不正に操作されてしまう可能性があります。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

SugarCRM Inc. が提供する「SugarCRM」は、顧客管理を行うソフトウェアです。「SugarCRM」には、オープンソース版と有償版があります。

「SugarCRM」には、データベースと通信する際の処理に問題がある、SQL インジェクション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、「SugarCRM」の管理者権限が攻撃者に取得され、「SugarCRM」上に登録されている個人情報が入り、データが削除されたりするなど、データベースを不正に操作されてしまう可能性があります。

最新情報は、次の URL を参照下さい。

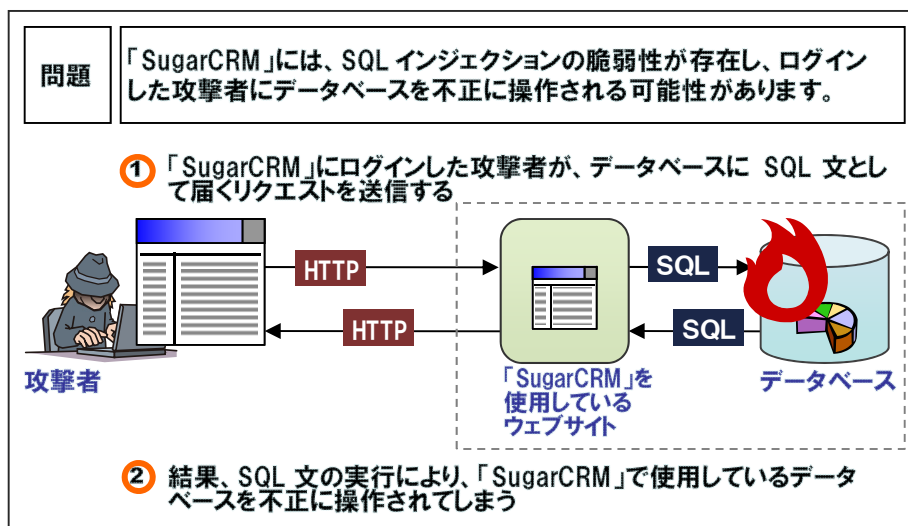
<http://jvndb.jvn.jp/jvndb/JVNDB-2009-000056>

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、2009年6月29日に以下の報告者から 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、2009年8月24日に公表したものです。

報告者:三井物産セキュアディレクション 寺田 健 氏

2. 脆弱性による影響

「SugarCRM」によって構築されたウェブサイトが、ログインした攻撃者から SQL インジェクション攻撃を受けた場合、「SugarCRM」の管理者権限が攻撃者に取得され、「SugarCRM」上に登録されている個人情報が入り、データが削除されたりするなど、データベースを不正に操作されてしまう可能性があります。



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 checked="" type="checkbox"/> レベル II(警告) (4.0~6.9)	<input type="checkbox"/> レベル III(危険) (7.0~10.0)
本脆弱性の CVSS 基本値		6.5	

(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 checked="" type="checkbox"/> 単一	<input type="checkbox"/> 不要
C: 機密性への影響	<input type="checkbox"/> なし	<input checked="" type="checkbox"/> 部分的	<input type="checkbox"/> 全面的
I: 完全性への影響	<input type="checkbox"/> なし	<input checked="" 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 checked="" type="checkbox"/> 部分的	<input 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

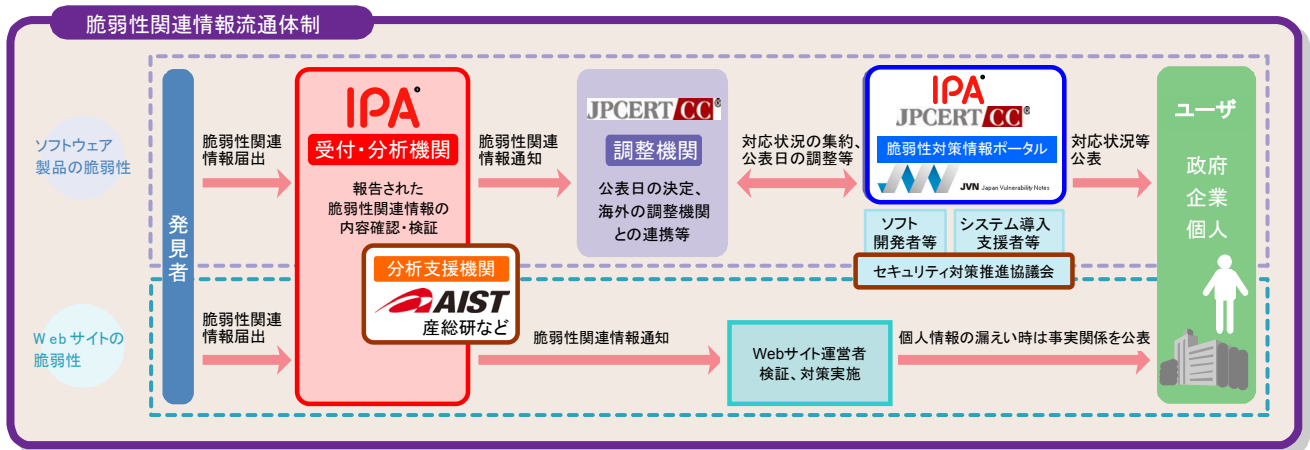
5. 本脆弱性の CWE³分類

本脆弱性の CWE 分類は、「SQL インジェクション (CWE-89)」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 山岸/渡辺
 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/大海
 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/SeverityCVSS2.html>

³ Common Weakness Enumeration. 共通脆弱性タイプ一覧。 <http://www.ipa.go.jp/security/vuln/CWE.html>