

Cisco Emergency Responder 盲目 SQL インジェクション脆弱性

| | | |
|--------|--|--------------------------------|
| Medium | アドバイザリーID : cisco-sa-20170906-cer | CVE-2017-12227 |
| m | 初公開日 : 2017-09-06 16:00 | |
| | バージョン 1.0 : Final | |
| | CVSSスコア : 5.4 | |
| | 回避策 : Yes | |
| | Cisco バグ ID : CSCvb58973 | |

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco Emergency Responder のための SQL データベースインターフェ이스の脆弱性は盲目 SQL インジェクション 攻撃を行なう認証される、リモート攻撃者可能にする可能性があります。

脆弱性は保護フィルターをバイパスする SQL クエリで使用されるユーザが指定する入力を検証する失敗が原因です。攻撃者は SQL 文を含む巧妙に細工された URL の送信によってこの脆弱性を不正利用する可能性があります。エクスプロイトは攻撃者がデータの統合に影響を与えるいくつかのデータベーステーブルの Modify エントリが表示するようにする可能性があります。

次のリンクはその他の情報を提供します:

https://www.owasp.org/index.php/SQL_Injection

この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170906-cer>

該当製品

修正済みソフトウェア

この脆弱性は Cisco Emergency Responder に影響を与えます。該当するソフトウェア リリースについての情報に関しては、このアドバイザリーの上で Cisco バグ ID を参照して下さい。

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

改訂履歴

| Version | Description | Section | Status | 日付 |
|---------|-------------------------|---------|--------|-------------------|
| 1.0 | Initial public release. | | Final | 2017-September-06 |

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。