GRANDIT におけるセッション管理不備の脆弱性について

ＧＲＡＮＤＩＴ株式会社
公開日　2020 年 2 月 28 日

平素より GRANDIT をご愛顧いただき、誠にありがとうございます。
この度、GRANDIT において、脆弱性が存在することが判明いたしました。
つきましては、現在 GRANDIT をご利用のお客様におかれましては、下記詳細内容を
ご一読頂き、リスク回避のための対応策の実施をお願い申し上げます。

1. 脆弱性の概要

セッション管理不備における脆弱性の問題が確認されました。
※3-2.に回避対応策を示していますので、導入パートナーにご相談の上、対応を
ご検討ください。

2. 脆弱性のもたらす脅威

悪意のあるサイト利用者が、ユーザ（被害者）のログイン時に取得したセッション ID を使い画面にアクセスすることができる。

3. 該当システム・パッチ情報、対策

3.1 該当バージョン・対策パッチ

製品名	バージョン	パッチ情報
GRANDIT	Ver.1.6	V160200228_K01
GRANDIT	Ver.2.0	V200200228_K01
GRANDIT	Ver.2.1	V210200228_K01
GRANDIT	Ver.2.2	V220200228_K01
GRANDIT	Ver.2.3	V230200228_K01
GRANDIT	Ver.3.0	V300200228_K01

3.2 対応策

前述のパッチ情報に基づき、GRANDIT 導入パートナーを通じて、パッチプログラムを入手してください。
なお、適用作業に関しましては、お客様の構築環境に依存する場合もあるため、一度 GRANDIT 導入パートナー様にご相談ください。

4. 関連情報

JVN#73472345　セッション管理不備の脆弱性

5. 更新履歴

・2020 年 2 月 28 日　新規掲載

・2020 年 3 月 2 日　関連情報を追記

6.　お問合せ先

本件についてご不明な点がございましたら、下記までお問い合わせください。

GRANDIT 株式会社　マーケティング担当　E メールアドレス：marketing@grandit.jp

以上