機密性1（低）情報
（重要インフラ事業者等への配布可）

令和5年10月18日

# ノースグリッド社製ProselfのXML実体参照（XXE）に関する脆弱性（第2版）

警察庁サイバー警察局
情報技術解析課
サイバーテロ対策技術室

※ 初版からの変更点を下線又は取り消し線で表示

# 1. 概要

- 2023年10月10日、株式会社ノースグリッドはオンラインストレージ構築パッケージ製品「Proself」に、XML外部実体参照（XXE）に関する新たなゼロデイ脆弱性があることを公開［7.参考（1）］
- 同社は本脆弱性の悪用を含む一連の攻撃を確認（攻撃を受けた場合、Proselfのアカウント情報を外部へ送信し、攻撃者はその情報を元に不正ログインを試行）
- 同社は脆弱性を悪用する攻撃を受けたかどうかの確認手順及び脆弱性が修正されたバージョン等をリリースするまでにすべき暫定対応の方法を提供し、脆弱性の悪用の有無に関わらず暫定対応が必要と注意喚起

# 1. 概要

- 2023年10月17日、同社はProselfの一部製品について本脆弱性を修正したバージョンをリリース [7.参考(1)]

# 2. Proselfについて

- ノースグリッド社製Proselfはインターネット経由でのファイルの保管や受け渡しを行うためのオンラインストレージを構築することができるソフトウェアであり、国内の企業、大学及び官公庁等で導入

# 3. 影響範囲

- ~~ノースグリッド社が公開している情報によると本脆弱性は現在リリースされている全てのバージョンのProselfが、対象~~
- ノースグリッド社が公開している情報によると本脆弱性の影響を受ける製品・バージョン及び脆弱性が修正されたバージョンは以下のとおり。

| 影響を受けるバージョン | 脆弱性に対応したバージョン |
|---|---|
| Proself Ver5.62 以下 | Proself Ver5.63 |
| Proself Gateway Edition Ver1.65以下 | 今後リリース予定 |
| Proself Mail Sanitize Edition Ver1.08以下 | |

※最新の情報及び詳細については、ノースグリッド社等のウェブサイト[7.参考(1)～(2)]を参照

# 4. 攻撃の発生状況

- ノースグリッド社は10月4日時点でこの脆弱性を悪用した攻撃の発生を確認

# 5. 攻撃の有無の確認

- ノースグリッド社は本脆弱性を悪用した攻撃の有無の確認方法として、以下を提示[7.参考(1)]
- 指定されたコマンドでアクセスログを検索して攻撃の有無を確認
- コマンド実行時に出力がある場合は攻撃を受けた可能性があるため、メール又はお問い合わせフォームで同社へ連絡
- JPCERT/CCが不正アクセス元のIPアドレスの情報を公開しており、同社の注意喚起に記載されている手順と合わせてこのIPアドレスに基づく攻撃の有無の確認を行うことを推奨[7.参考(1)～(2)]

# 6. 対策

- 脆弱性が修正されたバージョンがリリースされた製品は速やかに更新する。
- 脆弱性が修正されたバージョンがリリースされていない製品はリリースされ次第更新を行い、それまでの間は[7. 参考(1)]に記載の同社から提供されるファイルを適用することによる暫定対応を実施する(攻撃の有無に関わらず対応が必要)。
- [5. 攻撃の有無の確認]で攻撃を受けた可能性があると判明した場合は、Proselfが動作しているサーバ上の不正プログラムの有無やProselfにユーザがアップロードしたファイルの窃取の有無等の侵害状況の確認に加えて、ネットワーク内の別のサーバやネットワーク機器等が侵害されていないかを確認する。

# 7. 参考

(1)[至急]Proselfのゼロデイ脆弱性による攻撃発生について
https://www.proself.jp/information/153/
※17日付でノースグリッド社が製品アップデート及びリリース情報を更新

(2)ProselfのXML外部実体参照(XXE)に関する脆弱性を悪用する攻撃の注意喚起
https://www.jpcert.or.jp/at/2023/at230022.html
※18日付でノースグリッド社の公開した製品アップデート及びリリース情報を更新

# 8. 変更履歴

- 10月12日　初版
- 10月18日　第2版

1. 概要

一部製品の修正プログラムがリリースされた旨を追記

3. 影響範囲

影響を受ける製品・バージョンについての修正情報を追記

6. 対策

一部製品の修正プログラムがリリースされた旨を踏まえて製品の更新についての説明を追記

7. 参考

参考文献の更新状況を追記