NTT DATA
NTTデータ 先端技術株式会社

Splunk の管理項目における任意のファイルを表示可能な脆弱性に関する検証レポート

2012/9/7
NTT データ先端技術株式会社
辻　伸弘
小松　徹也
小田切　秀暁

【概要】

Splunk に、Splunk 動作権限で管理項目における任意のファイルを表示可能な脆弱性が存在することが発見されました。Splunk とは、アプリケーション、サーバ、ネットワーク機器のデータにインデックスをつけることで、IT インフラのイベントを、リアルタイムで検索・分析することができるソフトウェアです。

今回、この Splunk の管理項目における任意のファイルを表示可能な脆弱性の再現性について検証を行いました。

【影響を受けるとされているシステム】

- Splunk 4.3.3 およびそれ以前

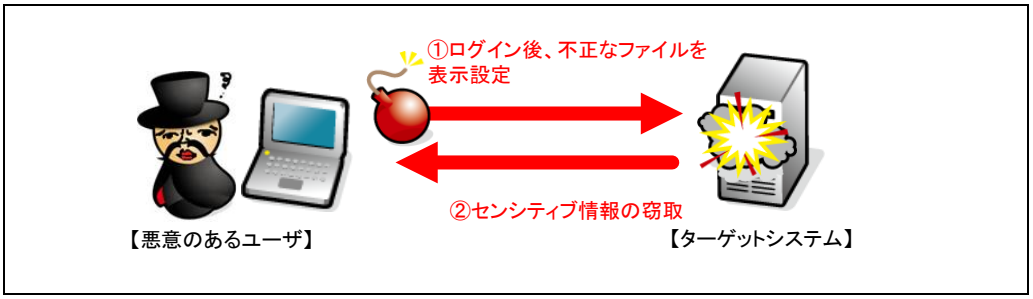
【対策案】

2012 年 9 月 7 日時点において、Splunk 社から本脆弱性を修正するバージョンはリリースされておりません。また、公開された脆弱性情報によると Splunk 社は本脆弱性を脆弱性と判断していないため、修正されない可能性があります。
この脆弱性を利用するには、「Admin」ロールの権限を有するユーザで Splunk へのログインが可能であることが必須条件となります。
そのため、今一度、Splunk のアカウントに脆弱なパスワードが設定されていないこと、アカウントへ付与する権限が適切であることを確認してください。さらに、必要に応じ強固なパスワード設定、適切な権限付与設定を実施していただくことが推奨されます。
また、Splunk に接続可能なアクセス元の制限を実施していただくことも併せて推奨されます。
さらに、Splunk を適切な権限で動作させることにより、攻撃成立時の表示対象ファイルを制限することが可能です。適切な権限にて Splunk を稼働させることも併せて推奨いたします。

なお、Splunk 社から本脆弱性を修正したバージョンがリリースされた際にはご利用環境への影響を確認の上、アップデートいただくことを推奨いたします。

Splunk ダウンロードサイト
http://www.splunk.com/download?r=header

【検証イメージ】



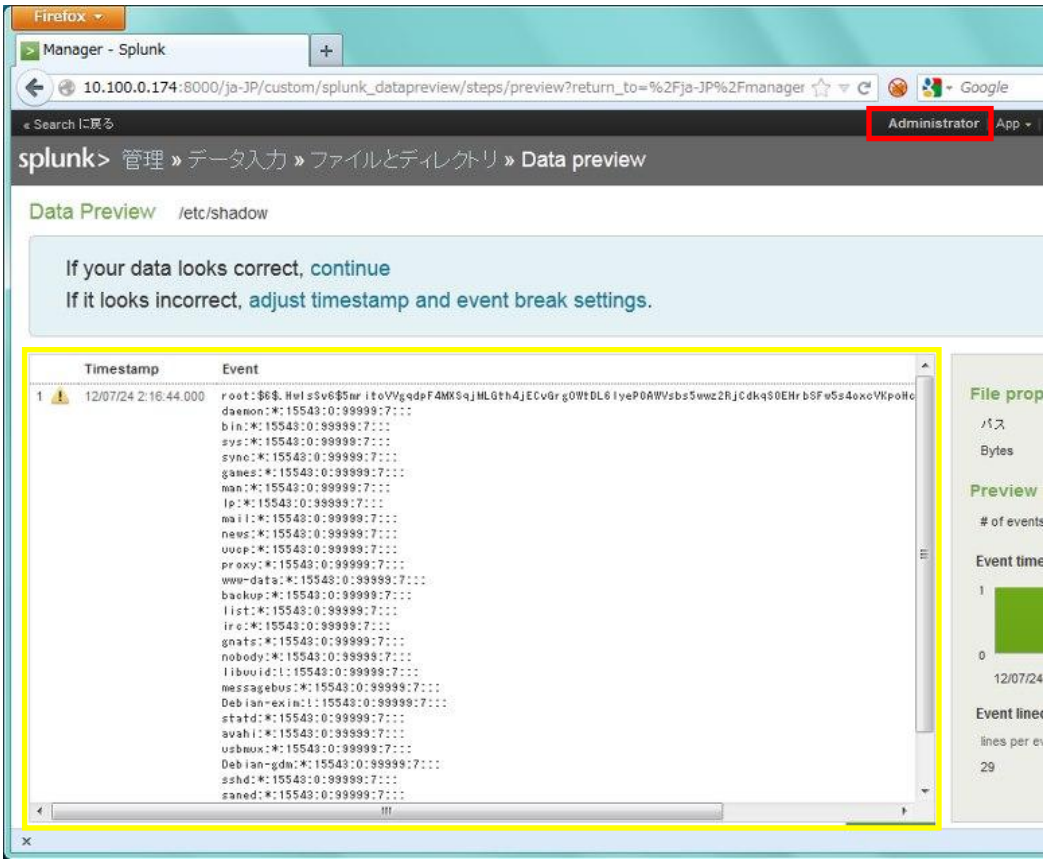
NTTデータ 先端技術株式会社

【検証ターゲットシステム】
Debian 6.0.5 上の Splunk 4.3.3

【検証概要】
Splunk に管理者権限ユーザでログイン後、ファイルパスを設定することで、任意のファイルを表示します。表示させるファイルは、「/etc/shadow」ファイルです。
※本脆弱性は、Splunk にログインできることが前提条件です。

【検証結果】
下図は、Splunk の管理設定画面です。赤字で囲まれている部分が示すように、Splunk に管理者権限でログインしています。
黄線で囲まれている部分の示すように、画面上には、Splunk の設定ではなく、「/etc/shadow」の内容が表示されていることからセンシティブ情報の窃取に成功したと言えます。

センシティブ情報「/etc/shadow」の窃取



＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ先端技術株式会社
セキュリティ事業部　営業担当　サービス企画戦略グループ
TEL：03-5859-5422
http://security.intellilink.co.jp