ICSソフトウェアにおける既知の脆弱性の特定と対処

要約

産業制御システム（ICS）は世界中で数多くの重要インフラおよび製造能力をサポートしているため、この分野でのソフトウェアの信頼性とセキュリティは大いに重要になります。

このケーススタディーでは、Synopsys 社のスタッフがインターネットからダウンロードして解析した、ある ICS 関連のソフトウェア開発キットに注目します。Synopsys 社は、ソフトウェアコンポジション解析を使用していればリリース前に取り除けていた可能性のある既知の脆弱性を、サードパーティー製のコンポーネントから何百も発見しました。

ソリューションの評価

今日のソフトウェアアプリケーションのおよそ 70%～90% がサードパーティー製のライブラリを使用しているという事実を考えると、ソフトウェアコンポジション解析は重要です。サードパーティー製コンポーネントのユーザーは、自分たちが使用するコンポーネントが安全であるかどうかを確認することに労力を割くことがほとんどありません。これは、セキュリティと品質のテストは上流の責任であると間違って想定しているためです。ソフトウェアコンポジション解析技術を適用すると、ソフトウェア内で使用されているサードパーティー製コンポーネントが安全であることを確認できるため、不必要なセキュリティリスクに労力を割かれることがありません。

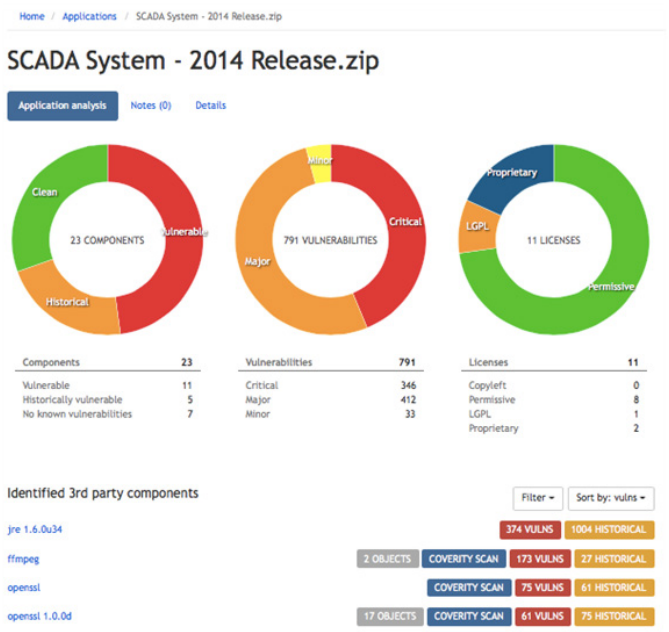
Protecode Supply Chain™ は、バイナリパッケージ内に含まれるサードパーティー製コンポーネント（および、その場所とバージョン）の包括的な部品表を提供することで、ソフトウェアコンポーネントのテストにかかる労力を軽減します。Protecode Supply Chain™ の解析エンジンは、米国の NIST NVD（NIST National Vulnerabilities Database）を初めとするさまざまなデータベースを使用して、各サードパーティー製コンポーネント内に存在する既知の脆弱性を列挙します。見つかったすべての既知の脆弱性に対し、Protecode Supply Chain™ は自身の CVE（Common Vulnerabilities and Exposures）番号を割り当て、この番号から、その脆弱性の詳細と重要度が分かります。

発見フェーズ

Synopsys 社のエンジニアリングとサポートのスタッフは、定期的に、バイナリパッケージを取得し、その内容を自身のクラウドサービスにアップロードすることで、Protecode Supply Chain™ をテストします。このスキャンの結果を解析することで、Protecode Supply Chain™ の有効性を判定するだけでなく、その結果を評価し、重要な発見があった場合は、解析したバイナリパッケージの開発者に報告します。

2014 年、Synopsys 社のエンジニアは、ある SCADA (Supervisory Control And Data Acquisition) ソフトウェアパッケージをそのベンダーの開発者 Web サイトからダウンロードしました。この Web サイトには、世界中で 20,000 を超えるユーザーがライセンスを受けており、その代表的な顧客として、空港や水管理などの重要インフラ分野がいくつも含まれていると書かれていました。

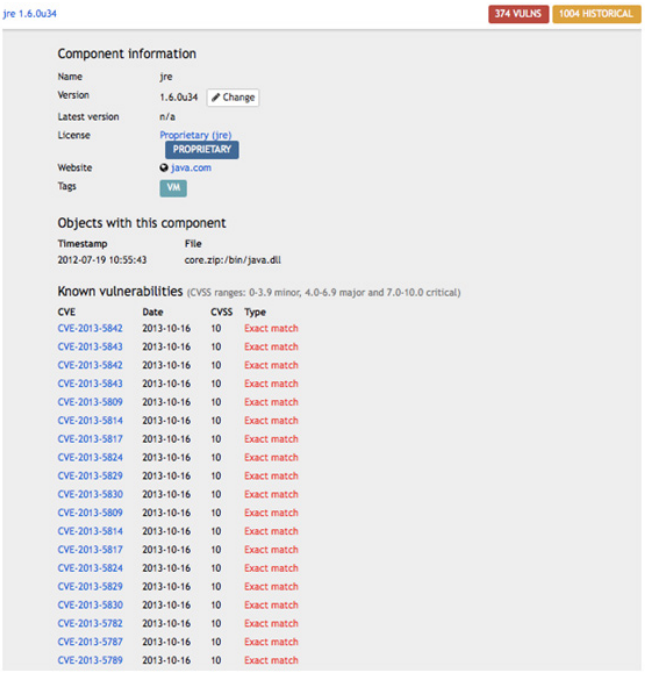
ダウンロードしたソフトウェアパッケージをスキャンすると、700 を超える既知の脆弱性がその製品に影響していたことが発見されました。



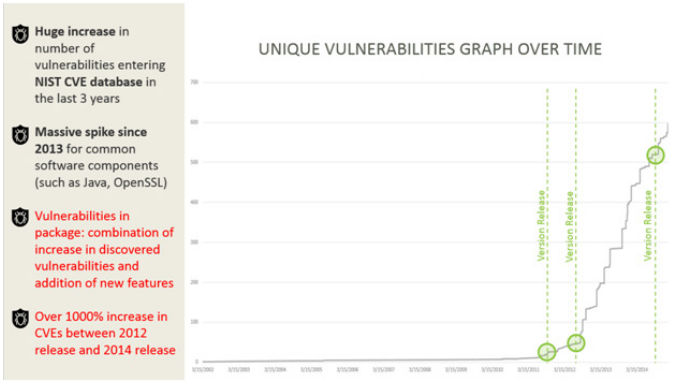
これらの脆弱性のうち、300 を超えるものが「重要」でした。この結果は主に、米国の NIST NVD（National Vulnerability Database）で使用されている評価システムによるものです（https://nvd.nist.gov）。

主に NIST NVD が、Protecode Supply Chain™ に CVE を提供します。米国連邦政府が出資している MITRE 社（https://cve.mitre.org）は、CVE をまとめ、脆弱性の詳細を明記し、重要度（0 から 10 まで）を割り当てています。7.5 から 10 までの重要度は評価システムにより「重要」であると見なされます。これはつまり、その脆弱性が認証なしでリモートから実行可能であることを意味します。

SCADA システム内の Java パッケージ（jre 1.6.0）には 300 を超える既知の脆弱性が含まれており、そのうち、150 を超える脆弱性が 7.5 から 10 までの重要度でした。



このパッケージをさらに解析し、最古のコンポーネントから最新のコンポーネントまで、時間経過による脆弱性の数をグラフ化しました。その結果は非常に驚くべきものでした。



縦軸は SCADA パッケージに影響する脆弱性（CVE）の数を示し、横軸は時間を表します。グラフに示されるとおり、システムに影響する脆弱性の数は 2012 年付近で急激に増加しています。

このベンダーの Web サイトには、2012 年から 2014 年の間に、3 つのリリース日が発表されていました。これらの日付は SCADA システムに影響する既知の脆弱性の急激な増加に一致します。つまり、(当社の解析によると)、明らかに、サードパーティー製コンポーネントを使用して製品を拡張したことが脆弱性の増加につながったことを示しています。

導入と実現された利益

当社はこのソフトウェア製造業者に連絡して、解析の結果を伝えました。ソフトウェアベンダーは最初ショックを受けた様子で、なぜこのような状況になったかを尋ねたところ、ソフトウェアに変更を実装したときと、サイバーセキュリティ上の脆弱性が増加したときが一致していると答えました。彼らがこの問題に気付かなかった理由は、ソフトウェアに含まれるサードパーティー製ライブラリを列挙するテストが彼らのテスト計画に含まれていなかったためです。

この SCADA システムのベンダーは当社が発見した問題に対処し、既知の脆弱性の数は 2 か月以内で合計 40 個までに大幅に減少しました。ほとんどの脆弱性は Java パッケージを最新のバージョンにアップデートするだけで対処できました。残りの 40 個の脆弱性は、その SCADA システム内のソフトウェアコンポーネントの 1 つが脆弱性のあるオープン・ソース・ライブラリに内部的に依存していたことが原因であり、そのコンポーネントの作者に対処してもらう必要がありました。

重要なことは、自分たちのソフトウェアの脆弱性を評価する必要があるという情報をソフトウェアベンダーに提供しただけで、彼らはすぐに対応して問題を修正できたと言うことです。しかしこれは、必ずしも、エンドユーザーが自分たちの SCADA システムを更新できたと言うことを意味しているわけではありません。なぜなら、そのようなシステムの多くは重要であり、このような変更を加えるためにオフラインにはできないためです。それでも、ソフトウェアベンダーは顧客のソフトウェアに影響する脆弱性があることを顧客に伝えることはできました。これにより、顧客は、ソフトウェアのアップデートやアップグレードがインストールされるまでの間、緩和手順を実装する機会を得ることができるのです。

まとめ

重要インフラを運営するために現代社会がテクノロジーにより依存するようになる中、制御システムソフトウェアにとって、セキュリティはより重要な課題となっています。開発ライフサイクルを通じて Protecode Supply Chain™ を使用すると、ICS 製造業者とエンドユーザーが制御システムソフトウェアの脆弱性を特定および軽減するのに役立ち、これにより、サイバー・フィジカルのプロセスでの全体的な安全性が保証されます。

SYNOPSYS®

www.synopsys.com/japan/software

日本シノプシス合同会社 営業本部 ソフトウェア インテグリティ グループ
〒158-0094 東京都世田谷区玉川2-21-1二子玉川ライズオフィス
TEL: 03-6746-3600 Email: sig-japan-sales@synopsys.com