Dell Technologiesのサプライチェーンセキュリティ: Secured Component Verification for PowerEdge

テックノート

Craig Phelps
Kim Kinahan
Mukund Khatri
Jason Young

概要

Secured Component Verification (SCV) は、セキュリティのさらなる強化を実現する、Dell Technologiesのサプライチェーンプログラムの重要な取り組みとして、まずDell EMC PowerEdgeサーバー全般を対象に提供が開始しました。

SCVによってお客様は、納品されたサーバーがセキュアであり、工場で生産された内部コンポーネントとその構成がお客様の指示通りであり、さらに、工場の出荷から納品までの間に第三者による改竄がない、という証明を得られます。

はじめに

Dell Technologiesは長年に渡り、安全な製品提供は、強力なサプライチェーン保証の仕組みによる強固なサプライチェーンから始まるものだと認識してきました。セキュリティ面の脅威がますます複雑化し、洗練されていく傾向にある中で、システムを保護する機能とその管理措置にも、それに見合った進化が求められています。攻撃の対象になり得る側面として、システムの製造時もしくは工場からの輸送時の、ハードウェアへの不正な物理アクセスやハードウェアの改竄（検出不能なマルウェアの混入など）が考えられます。工場を出荷されてから納品先へ到着までの間に起こり得る、偽造コンポーネントへのすり替え、マルウェアの混入、ファームウェアの改竄といった、サーバー製品がさらされる潜在的なセキュリティ上の脅威は、ユーザーには手の届かない脅威とも言えます。

昨今の企業や組織はサプライチェーンセキュリティの重要性をよく理解されており、それが購買の意思決定時の判断材料の一つにもなっています。このたびDell Technologiesは、業界全体で見られるお客様の懸念を最少化する方法として、まったく新しいサプライチェーンセキュリティの仕組みの提供を開始いたしました。対象はDell EMC PowerEdgeサーバーの全てのポートフォリオです。これは、納品されるハードウェアの健全性を向上するだけでなく、Dell Technologiesのサプライチェーンセキュリティの実践領域が拡大したことも意味します。

Dell Technologiesのセキュアなサプライチェーン

Dell Technologiesはお客様に信頼いただける製品の提供をおこなうため、多面的なアプローチでサプライチェーンの保護に取り組んできました。デスクトップPC、ノートPC、サーバー、データストレージアレイといった製品を問わず、新製品・新機能の開発、設計、プロタイプ化、実装、生産、お客様先への展開、メンテナンス、バリデーションは、すべてサプライチェーンセキュリティが最優先に考えられています。

サーバー製品は、開発ライフサイクルそのもの（製品設計、開発、製造、デリバリーまで）において全面的にサイバーセキュリティを強化し、プロセスの防御に努めています。

広範囲なサプライチェーン保証を実現するための、主な要素としては：

- 出荷物の保管追跡能力と、改竄防止型の梱包
- 生産現場での、第3者のアクセスエリアの制御と人員チェックの仕組み
- コードサイニング証明書の活用と、セキュアダウンロードの徹底
- 重要コンポーネントのメンテナンスにおける、チェーン・オブ・トラストチェーンオブ トラスト (信頼の連鎖)の活用
- 運用中のハードウェアへの不正侵入の検知能力と、輸送中の製品シャーシへの不正アクセスの記録（ログ）能力

Dell Technologiesは、サプライチェーンパートナー各社との信頼関係、そして自社およびサプライチェーンネットワーク全体における高い責任と健全性の基準により、お客様に信用いただける堅実な製造オペレーションを行っています。

上記のような手法は総じて、特に官公庁、銀行・金融、ヘルスケア、小売といった分野で、Dell Technologies製品の重要な差別化ポイントになっています。

Dell Technologies Secured Component Verification

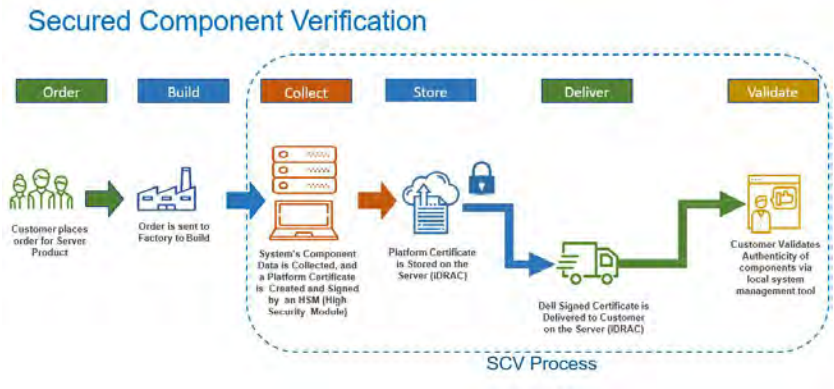
セキュリティのさらなる強化を実現する、Dell Technologiesのサプライチェーンプログラムの重要な要素の1つが、Secured Component Verification (SCV) です。現時点では、PowerEdgeサーバーポートフォリオの重要な選択肢として提供されていますが、今後、他の製品ラインでも採用される予定です。

Secured Component Verification for PowerEdgeを利用すると、納品されたPowerEdgeサーバーのハードウェア構成内容が、工場で生産された通りかどうかの証明を得られます。お客様にとっては、自社のミッションクリティカルなアプリケーションを担う堅実な基盤となるインフラについて、（構成がお客様の指定通りである点も含めて）そのハードウェアの健全性が最初に証明されるため、新規サーバーをより安心してデータセンターに導入できます。

IT管理者はSCVの利用で、納入されたサーバーの健全性をコンポーネントレベルでの検証が可能です。サーバーの構成が工場生産時と一致することを確認し、各コンポーネントとハードウェア構成が自社の指定通りであるか、そして工場から納品までの輸送期間で何か変更が加えられていないかを検証できます。もし、Dell Technologies工場を出荷してからこの検証までの間に、何らかのコンポーネントレベルの変更があった場合は、その対象項目が不一致だというレポート結果が出ます。つまり、お客様にとって予定通りの変更も、許可していない変更も、検知可能です。

工場では、各コンポーネント固有の識別IDと共に製造時のコンポーネント情報を収集して、その情報を暗号化された証明書として発行します。この証明書はサーバー内部にセキュアに保存され、製品の納品後にお客様が、証明書の内容と届いたサーバーの内部構成とを照合できるのです。照合には専用のアプリケーションが使われ、そのアプリケーションが、納品された製品の内部コンポーネントと、証明書内の固有の識別IDとを検証します。SCVでは、米国連邦政府の定めたサプライチェーンに関する暗号化の要件に適合した暗号化技術を採用しています。したがって、将来その要件が米国政府の標準規格となった場合にも、準拠できます。

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved.
Dell, EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries



アプリケーションによる証明

オーダー時にSCVライセンスが追加されたサーバーには、SCVで認証されたコンポーネントで構成されます。工場での製造段階で対象サーバーの重要な内部コンポーネントが分析され、コンポーネントのデータを含む固有のIDが付与されます。つまり、サーバー固有の暗号化された証明書内に、そのサーバー固有のハードウェア構成データが保存されるのです。このSCV証明書はDell Technologiesの証明書認証局（CA）の署名を受けた上でiDRAC内部に保存され、製品の納品後に、お客様がDell SCV Validationアプリケーションを使って読み出すことになります。証明書には鍵がかかり、当該サーバーはこの証明書を中に含んだ状態で、輸送され納品に至ります。

本番環境で新しいサーバーを展開するにあたり、お客様がサーバーの起動に先立ってSCV Validationアプリケーションを走らせれば、手元のサーバーのハードウェア構成と、Dell Technologies工場で生産時に収集された構成データとが、比較されます。このアプリケーションによる検証の結果は、完全な一致か、あるいは不一致のコンポーネントのリストとなります。

結論

IT管理者は、Secured Component Verification (SCV) の利用により、Dell Technologiesが工場で生産した内容を検証することはもちろん、工場出荷からお客様の納品先への輸送段階で起きたハードウェアの変更を（予定通りの変更と意図しない変更のどちらも）すべてトラックできます。

SCVにより、IT運用チームとセキュリティチームの双方が、新たに納品されたシステムのコンポーネント構成は指定通りである保証を得られ、同時にサイバーセキュリティの潜在的リスクを低減できます。サーバーインフラのセキュリティ面の保証と安心についてはDell Technologiesにご支援させていただき、お客様自信は、より多くの時間をビジネス成果に直結する活動に費やしていただけます。

PowerEdge DfD Repository
For more technical learning

Contact Us
For feedback and requests

Follow Us
For PowerEdge news

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved.
Dell, EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries