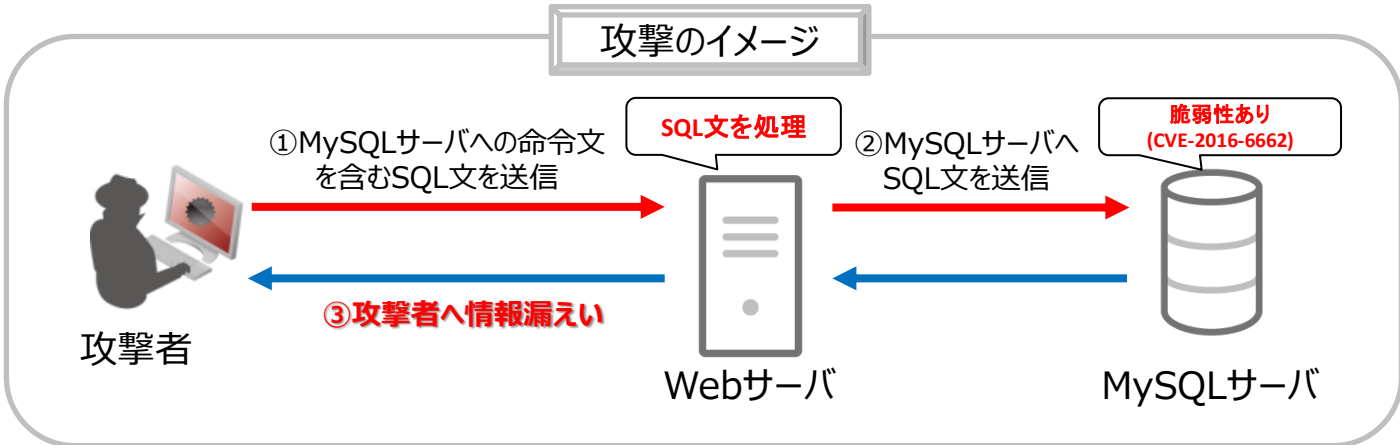


MySQLのゼロデイ脆弱性に注意！ リモートから管理者権限でサーバを制御される危険が！

世界で大きなシェアを持つオープンソースのレーショナルデータベース管理システム (RDMS) 「MySQL」にリモートからコード実行が可能な脆弱性があることが公表されました。

SQLサーバ内に不正プログラムを侵入させたり、データの窃取を行える「MySQLのゼロデイ脆弱性」への対処はお済みでしょうか。**現時点では修正プログラムは公開されていないので、早急に対策が必要です。**



脆弱性に関する情報

影響範囲	<ul style="list-style-type: none">MySQLの最新版を含む5.7系、5.6系、5.5系の全バージョンMySQLの派生DBである、「PerconaDB」や「MariaDB」にも影響(パッチは公開済み)
脆弱性の概要	<ul style="list-style-type: none">脆弱性番号：CVE-2016-6662CVSSスコア：7.9脆弱性を持つMySQLサーバに任意のSQL文を実行させることで、攻撃者が管理者権限で任意のコードを実行することが可能。

**MySQLのセキュリティパッチはまだリリースされていません！
Deep Securityの仮想パッチはもう対応しています！**

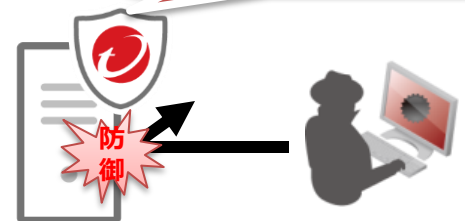


Trend Micro Deep Security™

Deep Securityの**仮想パッチ**技術を用いたIPS/IDS(侵入防御)機能は、今回のMySQLのゼロデイ脆弱性(CVE-2016-6662)に対応済みです。

ルールID : 1007950
ルール名 : Oracle MySQL Remote Code Execution Vulnerability (CVE-2016-6662)

サーバにDeep Security エージェントをインストール！
仮想パッチでブロック！



脆弱性を利用した攻撃と対策

今回、MySQLに存在することが公表された、リモートからコード実行が可能な脆弱性に関しては、既に攻撃手法のPoCも確認されています。この脆弱性を悪用する攻撃者はSQLサーバ内に不正プログラムを侵入させたり、データの窃取を行える可能性があります。現時点でこの脆弱性に関するMySQLの修正プログラムは公開されておらず、いわゆる**ゼロデイ状態**となっています。

トレンドマイクロではこの脆弱性に対応するため、**Trend Micro Deep Security**をおすすめしています。

Trend Micro Deep SecurityのIPS/IDS(侵入防御)機能が持つ、仮想パッチ技術を用いることで、この脆弱性が存在するMySQLサーバを保護することが可能です。

また、この脆弱性を利用するためにはMySQLサーバのフロントに位置するWebサーバにSQLインジェクション攻撃を成功させる必要があります。Trend Micro Deep SecurityはWebサーバへのSQLインジェクション攻撃も検知・防御することが可能です。

仮想パッチとは？

ネットワークレベルでパケットの中身を確認し、プロトコル違反・シグネチャベースによるマッチングを行います。パターンにマッチングしたパケットを「脆弱性を狙った攻撃パケット」と判断し、検知・ブロックします。結果、仮に脆弱性が存在しているシステムでも、そこを狙った攻撃から保護されます。

～仮想パッチのイメージ～



トレンドマイクロの仮想パッチソリューション

サーバ用

**Trend Micro
Deep Security™**



<http://www.trendmicro.co.jp/tmds/>

クライアント用

**Trend Micro™
Virtual Patch for Endpoint
(旧 Trend Micro 脆弱性対策オプション)**



<http://www.trendmicro.co.jp/jp/business/products/tmvp/index.html>