KernelCare

KernelCareの仕組み

リブートは被害を与えます

サーバをリブートすると、顧客に被害を与え、またあなたにも被害を与えることになります。ピークタイムのサービスへの影響を最小限に抑えるために、多くの場合それは深夜に行われます。あなたとあなたのビジネスにダウンタイムを強制することになり、サーバのリブートが完了するまでに15分以上かかることがあります。
パフォーマンスが安定し、すべてのサービスが実行されていることを確認するまでにはさらに時間がかかります。リブートは頻繁に行いたいことではありません。しかしリブートがカーネルセキュリティの脆弱性に対するパッチを適用する唯一の方法だったのです。

これまでは...

今やKernelCareがあるのです。リブートせずに自動的にカーネルセキュリティの脆弱性を修正します。ダウンタイムもサービスの中断もありません。

KernelCare

KernelCare

パッチの準備

私たちのカーネルチームはセキュリティメーリングリストをモニターしています。サポートしているカーネルに影響を与える脆弱性が発表されたら、すぐにパッチを準備します。そのカーネル用の各パッチをコンパイルし、それを私たちの配布用サーバに展開します。
サーバ上で実行されているKernelCareエージェントプロセスは4時間ごとに配信サーバと同期およびチェックを行います。アクティブなカーネルに新しいパッチが利用可能な場合、エージェントはそれをダウンロードして、実行中のカーネルに適用します。あなたのカーネルはまた安全となるのです。

KernelCare

パッチの仕組み

脆弱性を発見したら、「パッチ」を作成します。これは安全でないカーネルコードに、安全で機能的に同等な代替品としてのパッチを当てたコードです。

最も単純な場合では、パッチをあてるとはコードの一行の修正を意味することがあります。その他の場合、欠けているチェックの追加、データ構造または機能の変更など、より複雑な軽減策が必要になることがあります。

変更された内容とその適用方法に関する情報を追加し、通常どおりにパッチを適用したコードをコンパイルします。

特別なカーネルモジュールがパッチを適用します

パッチを適用するために、特殊なKernelCareカーネルモジュールが使用されます。それはアップデートをカーネルアドレススペースへロードし、再配置を設定し（すなわち、オリジナルのカーネルコードとデータへの参照を修正し）、実行パスをオリジナルのコードブロックからアップデートされたコードブロックへと安全に切り替えます。変更を正しく適用することが重要であり、KernelCareはそれを正しく実行することができます。新しいバージョンに切り替えると、CPUはオリジナルのコードブロックを実行しないことを確認します。

カーネルメモリを割り当て、そこに新しく安全なコードをロードします

「安全」な状態にあるすべてのプロセスを一時的にフリーズさせます。

オリジナルの機能を変更して新しく安全なコードへとジャンプし、古い（脆弱な）コードが実行されないようにします。

すべてのプロセスの凍結を解除して再開します。

KernelCareはパッチ適用を超高速化させます

パッチを適用する瞬間的なアップデートプロセスはダウンタイム、サービスの中断、またはパケットのドロップがないことを意味しています。すべての脆弱性がなくなり、すべてが以前と同じように機能し続けます。

KernelCare:
リブート不要の自動セキュリティアップデート

KernelCareに関するより詳細な情報や無料評価については、
日本国内正規代理店 GDEPソリューションズ株式会社
までご連絡下さい。
電話：03-5802-7050　E-mail：kcsales@gdep-sol.co.jp

KernelCare