マネージドセキュリティサービス 最前線
第9回 ー 実例ベースで考える ー

独自シグネチャによる脅威への緊急対応と脆弱性マネジメント

NTT コミュニケーションズ㈱　経営企画部
マネージドセキュリティサービス推進室長
与沢 和紀

NTT コムセキュリティ㈱
オペレーション＆コンサルティング部
羽田 大樹

日々の本来業務に追われるなか、毎日のように発見されるソフトウェアの脆弱性について、そのつど情報を追いかけて迅速に対応していくことは難しい。アップデートが公開されていないゼロデイ脆弱性の場合はなおさらである。ネットワークで攻撃を遮断して脅威を緩和する IPS や WAF といったセキュリティ製品もあるが、攻撃を検知するシグネチャがすぐにリリースされない場合もある。連載第 9 回となる今回は、このような脅威に対する対策の取り組み事例について紹介したい。

GNU bash 脆弱性（Shellshock）

2014 年 9 月 25 日の深夜 0 時ごろ、GNU bash に存在する脆弱性とその修正プログラムが世界に公開された。bash は Linux などの OS においてコマンドを実行するためのシェルプログラム（OS の一部としてプログラムの起動や制御などを行うプログラム）であり、他にも UNIX 系 OS、BSD 系 OS、Apple の OS X など、幅広く利用されている。Web アプリケーション等において bash を直接的、もしくは間接的に利用している環境では、外部からそのサービスの権限を用いてサーバを乗っ取ることができる危険な脆弱性である。

脆弱性の対応

深夜に脆弱性情報通知システムからメールでこの情報を入手した我々は、朝からこの脆弱性に対応するための詳細な情報収集に専念した。攻撃コードの入手や攻撃を再現する環境の準備、影響を受ける可能性があるお客様の把握など、役割を分担して今後の対応を判断できる材料を集めた。

すでに修正プログラムが公開されているため、適切に更新を行えば対策は完了するものの、即座に対応できるシステム管理者は多くない。また、脆弱性の影響を受ける可能性のあるシステムは広範囲に渡り、狙われた場合のリスクも高い。このことから、IPS や WAF といったセキュリティ機器での緩和策を検討することにした。実際に、我々の顧客にも脆弱性の影響を受けるサンプルのプログラムが残っていて、ただちに侵入可能であると判断できるサーバを 2 台発見した。急いで連絡し、即座にプログラムを削除してもらった。

並行して IPS や WAF の各製品ベンダーに、公式シグネチャのリリース予定を確認した。一部の製品では夜に提供できるという返答もあったが、ほとんどは未定という回答であったため、独自のシグネチャを作成することにした。IPS や WAF で検知するための独自シグネチャの作成は、L3（エルサン）と呼ばれるセキュリティのプロフェッショナル部隊が担当している。

検証はスムーズに完了し、攻撃を正しく検知、遮断できることはすぐに確認できた。ところが、いくらセキュリティが重要とはいえ正しい業務通信まで誤って遮断してしまうことは許されない。シグネチャを適用する際、最初のうちは遮断をせずに様子を見るのが通常であるが、このような脆弱性対応の場合は時間が限られている。そのため、我々が管理しているプロキシサーバのログを活用し、30 億以上のアクセスと照らし合わせた上で、正常な通信に該当パターンが含まれないかを確認した。ここで、一部のサイトへのアクセスにおいては、このロジックが正常通信にも適合してしまうことが判明したため、確実に攻撃と判断できるパターンと、正常な通信に適合しうるパターンの 2 種類のシグネチャを作成することで最適化を行った。13 時ごろには独自シグネチャが完成して、適用作業に取り掛かった。

さらなる脆弱性の公開

15 時過ぎに新たな情報を入手した。公式に提供された修正プログラムに不備があったという。さらに状況が悪いことに、この新たな脆弱性は修正プログラムが公開されていないゼロデイの脆弱性だという。ますます独自シグネチャの作成が重要な意義を持つようになった反面、現在

図 1　Shellshock 対応とシグネチャ提供の時系列

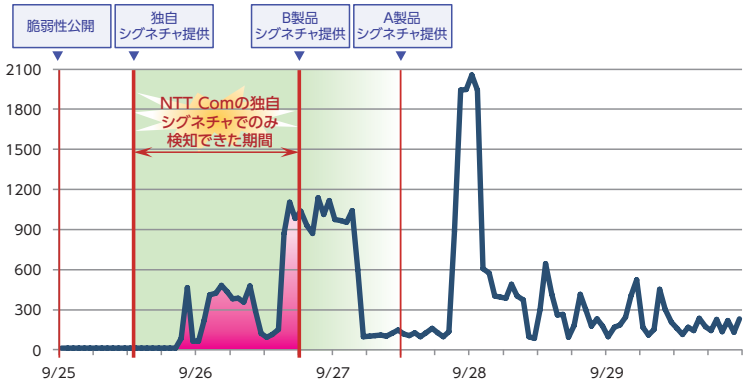

図 2　Shellshock に対する攻撃の検知数の推移

適用しているシグネチャは意味をなさなくなってしまうため、急いで新たな脆弱性の内容や攻撃コードを確認し、追加で検証を行った。結果的には、元の脆弱性も新しい脆弱性も同じロジックで防御できることが確認でき、方針を変更せずに対応を継続することができた。

独自シグネチャによる脅威への緊急対応を振りかえって

今回の Shellshock の対応の時系列は図 1 のとおりとなった。脆弱性が公開された当日中に独自シグネチャを提供したことで、製品ベンダーがシグネチャを提供していない 28 時間以上の期間においてもシステムを保護することができた。また、今回の攻撃の検知数は図 2 のとおり、シグネチャを適用して 7 時間後から攻撃を遮断し始めた。攻撃の内容を分析したところ、攻撃者がこの脆弱性を悪用する自動化ツールを作成して手当たり次第脆弱なサーバを探していたことが分かったが、それに先駆けて対策することができたのである。

Shellshock はメディアで大きく取り扱われたこともあり、お客様から多くのお問い合せを受けたが、すでにシグネチャを適用していると回答し、安心していただくことができた。

脆弱性マネジメントを考える

IPS や WAF の導入、その後のマネジメントは自社でも出来ると考えられるが、このような緊急の脆弱性対応の実施面までを考慮し、WideAngle のような専門の MSS 事業者への委託を真剣に考えるべきであり、その際、単にシステムの管理だけでなく、緊急対応の能力まで十分に比較したい。

また、自社システム全ての使用 OS、ミドルウェア及びオープンソースのアプリ機能の活用内容を日頃から把握し、重大な脆弱性情報が発出された場合の対応についても仕組みや体制を整えておく必要がある。本紙 8 月号の連載第 7 回にて触れたが、弊社と一部のグループ会社では「ISMP」（Information Security Management Platform）という脆弱性マネジメント（PDCA）を実現するプラットフォームサービスを開発／展開して、すべてのシステム管理者からセキュリティ管理者まで関係するプレイヤーが利用・連携して活用している。ISMP では、システムの脆弱性情報を自動的に収集し、各システムに必要な情報だけを抽出し、その管理者に自動通知する。その後、セキュリティパッチ適用等の必要な措置を完了するまでトラッキングし続けるため、脆弱性対応を徹底できる仕組みとなっている。併せて専門家により構成されるアドバイザリーチームがシステム管理者からの質問・相談に応える体制を整備している。今回の GNU bash 脆弱性（Shellshock）対応に際して、1 時間以内の使用システム把握と必要に応じた遮断、15 時間以内での 3 ケタを優に超える数のシステム全てに対する防御を完了できた。システムが多大で、システム毎に管理者を設置する状況における脆弱性マネジメントに頭を悩ませている企業も多いと思われるが、このような一元的な管理も抜本的な対策として検討してはと思う。

お問い合わせ先
NTT コミュニケーションズ㈱
経営企画部 マネージドセキュリティサービス推進室
E-mail：mss-sp-cp@ntt.com