NTTデータ・セキュリティ株式会社

DNS キャッシュポイズニング（汚染）の脆弱性に関する注意喚起

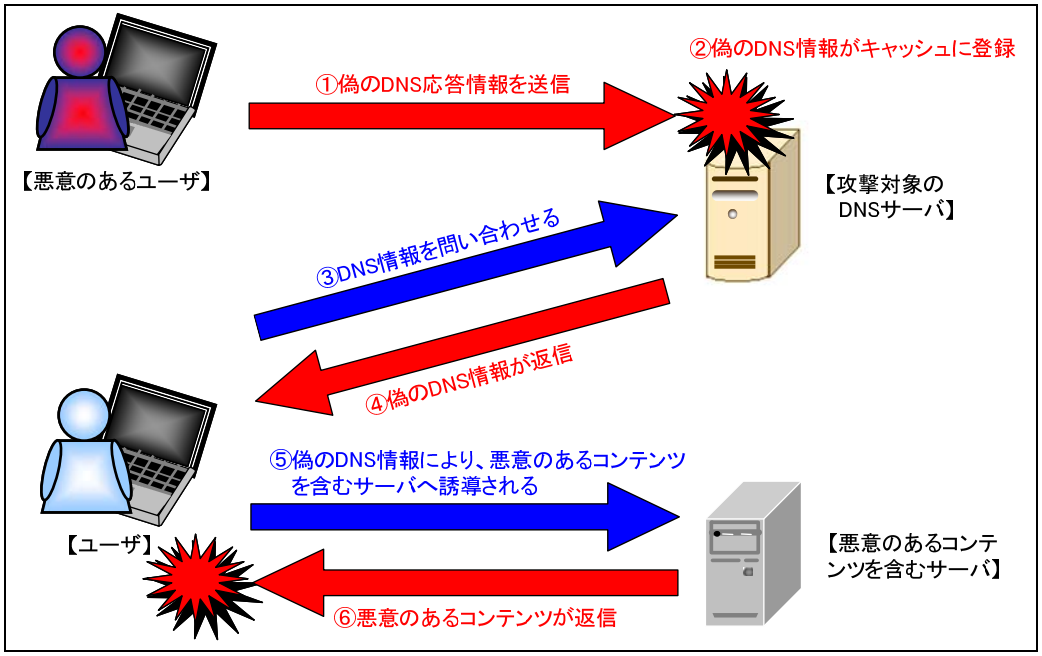
2008/7/25
診断ビジネス部
辻　伸弘
松田　和之

【概要】

複数の DNS サーバ製品の「DNS トランザクション ID」、及び、「UDP ソースポート番号」の使用方法に設計上の欠陥が存在し、DNS キャッシュポイズニングの脆弱性の影響を受けることが発見されました。
DNS キャッシュポイズニングとは、DNS サーバのキャッシュに偽装したドメイン情報を記憶させることを指します。想定される被害としては、悪意のあるユーザにより、不正なサイトに誘導され、フィッシング・ファーミングに利用されることが挙げられます。

この脆弱性は、「DNS トランザクション ID」の乱数が予測可能であること、「UDP ソースポート番号」が固定されていることに起因しています。
これにより、悪意あるユーザは、DNS サーバに偽装した応答情報を送信することにより、不正な IP アドレスを DNS サーバのキャッシュに登録することが可能となります。

【被害イメージ】



【DNS の仕組みと DNS キャッシュポイズニングによる影響】

DNS とは、ドメイン名と IP アドレスを相互に変換するシステムです。
コンピュータが他のコンピュータと通信するには、IP アドレスを使用します。ただし、IP アドレスは、数字の羅列であるため、人が覚えるのは困難です。そのため、人が覚えやすいドメイン名とコンピュータが利用する IP アドレスを相互に変換するシステムが考えられました。それにより、人が覚えづらい数字の羅列である「IP アドレス」を使用せずに、人の覚えやすい単語のようなアルファベットの組み合わせである「ドメイン名」を使用することが可能になりました。

以下に、ユーザが「www.nttdata-sec.co.jp」へアクセスする場合の流れを示します。
①ユーザは、DNS サーバにドメイン名「www.nttdata-sec.co.jp」の IP アドレスを問い合わせる
②DNS サーバは、「www.nttdata-sec.co.jp」の IP アドレス「211.129.14.134」を応答として返信
③ユーザは、DNS サーバから受け取った IP アドレス「211.129.14.134」宛へアクセス
④ユーザに「www.nttdata-sec.co.jp」のコンテンツが送信される

このように、ドメイン名と IP アドレスは対となっております。

以上を踏まえ、DNS キャッシュポイズニングの影響を受けた場合のアクセスの流れを示します。
①ユーザは、DNS サーバにドメイン名「www.nttdata-sec.co.jp」の IP アドレスを問い合わせる
②DNS サーバは、「www.nttdata-sec.co.jp」の偽の IP アドレス「悪意のあるコンテンツを含むサーバの IP アドレス」を応答として返信
③ユーザは、DNS サーバから「偽の IP アドレス」を受け取るため、正規の「www.nttdata-sec.co.jp」にアクセスしたつもりが、「偽の IP アドレス」宛へ誘導される
④ユーザに「悪意のあるコンテンツを含むサーバ」のコンテンツが送信される

【DNS キャッシュポイズニングの仕組み】

DNS サーバは、正規の応答であることを判断する際、「トランザクション ID」、及び、「UDP ソースポート番号」を利用します。
そのため、正しいトランザクション ID、及び、UDP ソースポート番号を含んだ偽装応答を送信されると、DNS サーバは、正規の応答であると判断し、不正なドメイン情報がキャッシュに登録されることとなります。

DNS サーバは、ユーザから指定されたドメイン情報が、自身のキャッシュに存在しない場合、外部の DNS サーバへ問い合わせます。
最終的に、指定されたドメイン情報を含む DNS サーバから応答を受け取り、要求したユーザにドメイン情報を返信します。この際、自身のキャッシュにドメイン情報を書き込みます。
次回、同様のドメイン情報が要求された際は、外部には問い合わせず、自身のキャッシュを参照し、ユーザにドメイン情報を返信します。

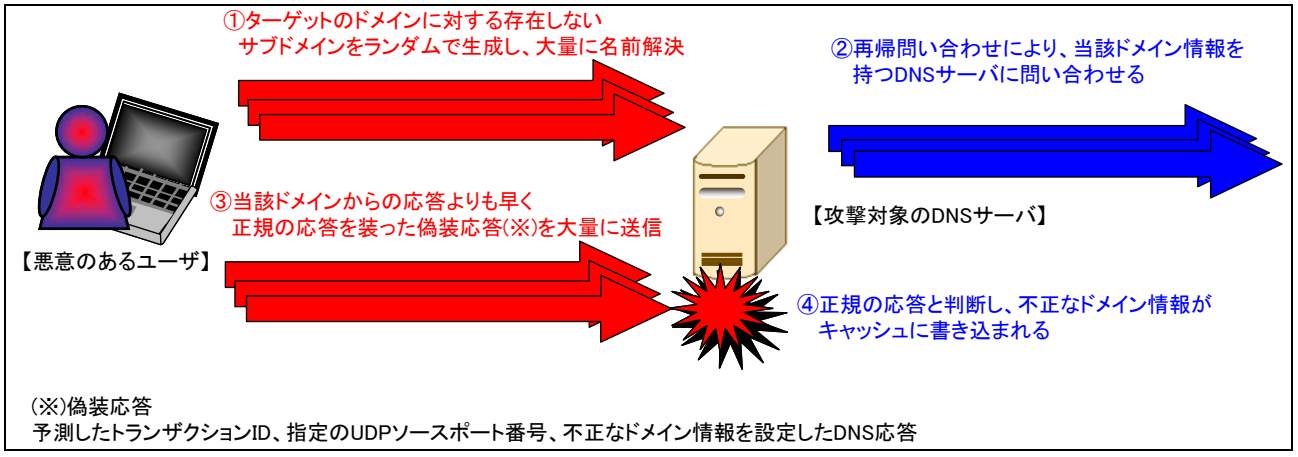
特定のドメインに対する DNS のキャッシュを汚染するためには、まず、ターゲットドメインに存在しないサブドメインの DNS 要求を行います。（DNS キャッシュポイズニングのイメージ①）

DNS 要求を受けた DNS サーバは、自身のキャッシュには存在しないため、外部へ DNS 要求を送ります。
（DNS キャッシュポイズニングのイメージ②）

悪意のあるユーザは、正規の応答よりも早く、予測したトランザクション ID、指定の UDP ソースポート番号、不正なドメイン情報を設定した偽装応答を、DNS サーバへ送信します。（DNS キャッシュポイズニングのイメージ③）

前述したとおり、DNS サーバは、トランザクション ID、及び、UDP ソースポート番号から、正規の応答であることを判断します。正しいトランザクション ID、UDP ソースポート番号である場合、不正なドメイン情報が DNS サーバのキャッシュに書き込まれます。（DNS キャッシュポイズニングのイメージ④）

【DNS キャッシュポイズニングのイメージ】



NTTデータ・セキュリティ株式会社

【影響を受けるとされているシステム】
ISC BIND の全てのバージョン（BIND 8 を含む）
Microsoft DNS サーバ
複数の Cisco 製品
複数の Juniper 製品（Netscreen 社製品を含む）
YAHAMA RT シリーズ
古河電工 FITELnet シリーズの一部

※なお、上記の影響を受けるとされているシステムは、現時点（7 月 25 日時点）のものであり、上記に記載のない製品も影響を受ける可能性があります。

【対策案】
各 DNS サーバ製品のベンダが提供する修正プログラムを適用することが推奨されます。
また、キャッシュサーバとしての機能（再帰問い合わせ）の必要性を確認し、不要であれば DNS 再帰問い合わせを無効化することが推奨されます。必要な場合は、DNS キャッシュサーバへの外部からのアクセス制限を実施することが推奨されます。

しかしながら、DNS プロトコルの実装には、以下の 2 つの欠陥が存在します。
①トランザクション ID が 16 ビットのみであること
②送信クエリに使用する UDP ソースポート番号が固定であること

修正プログラムを適用することにより、ソースポート番号の乱数の強度が上がり、ポート番号の予測が困難となります。ただし、攻撃が成功する確率が軽減されますが、依然、キャッシュポイズニングを受ける可能性は残ります。
そのため、根本的な解決を図るためには、DNSSEC を導入することが推奨されます。
DNSSEC とは、DNS 情報の通信において、電子署名を付加することにより、DNS 情報の改ざんを検出できるようにした DNS のセキュリティ拡張機能です。これにより、偽装された応答が送信された場合でも、不正な DNS 情報であると検出でき、DNS キャッシュポイズニング攻撃を防ぐことができます。

【確認方法】
以下の URL から、現在、お使いの DNS サーバが脆弱性の影響を受ける可能性があるかを確認することができます。
また、修正プログラムを適用後、脆弱性が修正されたかどうかの確認にも利用できます。

porttest.dns-oarc.net -- Check your resolver’s source port behavior | DNS-OARC
https://www.dns-oarc.net/oarc/services/porttest

【参考サイト】
JPCERT
http://www.jpcert.or.jp/at/2008/at080013.txt

US-CERT
http://www.kb.cert.org/vuls/id/800113

＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ・セキュリティ株式会社
営業企画部
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/