INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2008 年 9 月 18 日
独立行政法人 情報処理推進機構

DNS キャッシュポイズニングの脆弱性に関する注意喚起

－放置すれば情報漏えい～信用失墜に至る可能性も。
ウェブサイト運営者は早急に DNS サーバのパッチ適用や設定変更を！－

独立行政法人情報処理推進機構（略称：IPA、理事長：西垣 浩司）は、「DNS サーバに対する DNS キャッシュポイズニングの脆弱性」の届出が激増していることから、ウェブサイト運営者へ注意を喚起するとともに、DNS サーバのパッチ適用や設定変更を呼びかけます。

DNS(Domain Name System)[1]キャッシュポイズニング（汚染）の脆弱性に関して、2008 年 7 月に複数の DNS サーバ製品の開発ベンダーから対策情報が公開されています[2]。また、この脆弱性を悪用した攻撃コードが既に公開されていたため、2008 年 7 月 24 日、IPA はウェブサイト運営者へ向けて緊急対策情報を発行しました[3]。

しかし、この脆弱性に関して、「実際に運用されているウェブサイトの DNS サーバに対策が実施されていないのではないか？」という旨の届出[4]が昨今激増しています。

この脆弱性への対策を怠り悪用された場合、サイト運営組織内の利用者が、正しいウェブサイトの宛先を指定したにもかかわらず、知らぬ間に悪意のあるサイトに誘導され、金銭被害や個人情報漏えいの被害を受けてしまう可能性があります。結果として、サイト運営者は組織としての社会的な信頼の失墜や、経済的損失を被ることにもなりかねません。

これらのことから、IPA としては、改めて**ウェブサイト運営者、企業経営者に対して注意を喚起するとともに、DNS サーバのパッチ適用や設定変更の早急な実施を呼びかける**こととしました。

1.DNS サーバに対する DNS キャッシュポイズニングの脆弱性の届出状況

DNS サーバに対する DNS キャッシュポイズニングの脆弱性の届出は、図 1 に示すように 8 月 18 日の週から届出があり、9 月に入ってからは、毎週数十件にのぼっています（累計 204 件、9 月 18 日 12:00 現在）。通常の脆弱性の届出は、毎週 10～20 件程度であることから、DNS キャッシュポイズニングの脆弱性の届出件数が突出して激増していると言えます。

脆弱性が届出られたウェブサイトの運営者は、政府機関、地方公共団体、民間企業など広範囲に渡っています。社会的影響の大きいウェブサイトの DNS サーバについても多数の届出があり、各サイトの運営者は早急な調査と対策実施が必要です。

---

[1] コンピュータがネットワークのどこに接続されているかを示す IP アドレスという数字の集まりを、www.ipa.go.jp のような人に覚えやすいドメイン表記と対応させるための情報を管理する仕組みです。
[2] 脆弱性対策情報データベース JVN iPedia「複数の DNS 実装にキャッシュポイズニングの脆弱性」を参照ください。http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001495.html
[3] 複数の DNS 製品の脆弱性について。http://www.ipa.go.jp/security/ciadr/vul/20080724-dns.html
[4] ソフトウェア等の脆弱性関連情報に関する届出制度：経済産業省告示に基づき、2004 年 7 月より開始しました。IPA は届出受付・分析、JPCERT/CC は国内の製品開発者などの関連組織との調整を行っています。

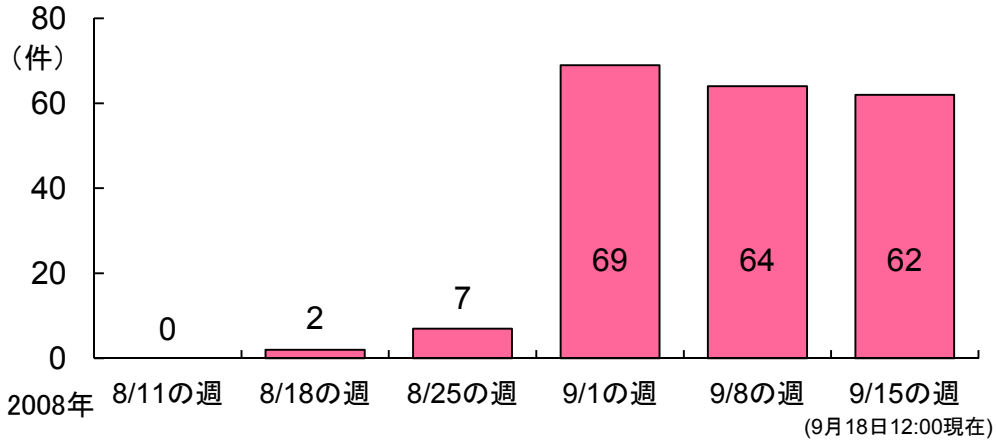

図 1.DNS キャッシュポイズニングの脆弱性の届出件数の推移

2. DNS キャッシュポイズニングの脆弱性の脅威

DNS には、検索した IP アドレスを一定期間記憶（キャッシュ）する仕組みがあり、DNS サーバ（DNS キャッシュサーバ）はその役割を担います。

DNS キャッシュサーバに DNS キャッシュポイズニングの脆弱性があり、これを利用した攻撃が行われると、正しい IP アドレスを検索できなくなります。その結果、ウェブサイトや電子メールなど、インターネット上で稼働している主要なシステムにおいて、正しい接続先に接続できなくなります。

ウェブサイトの場合、図 2 に示すように、利用者を偽のサイトに接続させることにより、パスワードやクレジットカード番号などの情報を盗まれる可能性があります。その他、メールの場合、メールを偽のサーバに配送させることにより、メールの盗聴・改ざんを受ける可能性があります。

これらの脅威は、実際に被害を受けている場合でも、利用者から見れば正常な場合と見分けがつかないため気付くことが困難、という特徴があります。

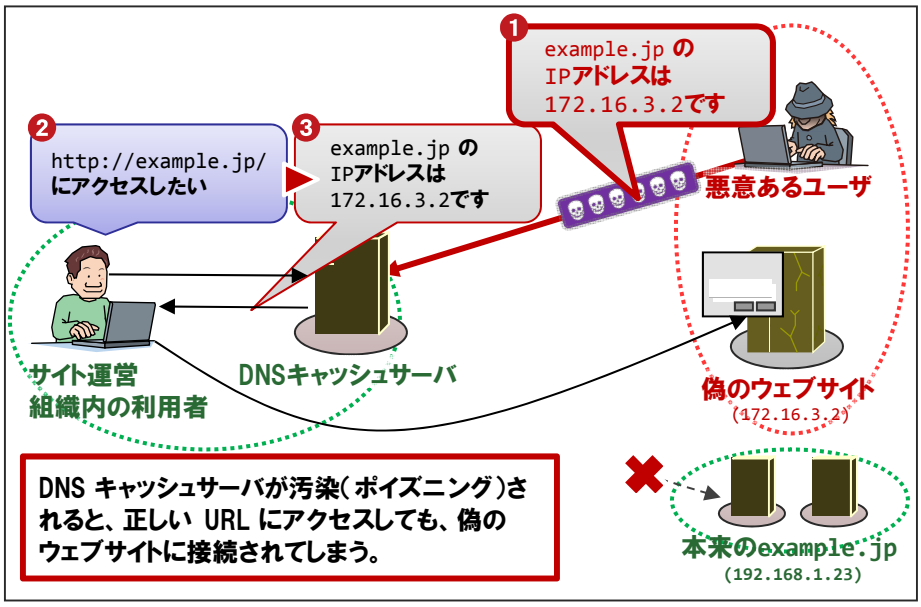

図 2.DNS キャッシュポイズニングの脅威例（ウェブサイトの場合）

3.脆弱性有無の調査方法

DNS キャッシュポイズニングの脆弱性の有無を確認するには、DNS サーバにおいて下記の 3 点を確認する必要があります。下記 3 点のうち、いずれかに該当する場合、利用している DNS サーバにパッチが適用されていないか、または、DNS サーバの設定に問題があります。

A. DNS 問い合わせに使用するポート番号がランダム化されていない。
B. DNS 問い合わせに使用する ID がランダム化されていない。
C. 外部からの再帰的な DNS 問い合わせに対して回答してしまう。

現在、これらを一度に確認する方法はありませんが、個別に確認するには下記の方法があります。

3.1 自組織の DNS キャッシュサーバに対して A.を確認する

DNS 問い合わせにおいて、ポート番号が十分にランダム化されていない場合、被害を受けやすくなります。

DNS-OARC[5]が提供するツール「porttest.dns-oarc.net」（英語）を使用すると、自組織の DNS キャッシュサーバに対して A.を確認することができます。

porttest.dns-oarc.net -- Check your resolver's source port behavior
https://www.dns-oarc.net/oarc/services/porttest

このツールによる確認は、OS のコマンドラインから行います。Windows の場合、下記のように nslookup コマンドを使用することで、確認が可能です。

「porttest.dns-oarc.net」を使用した A.の確認

```
> nslookup -querytype=TXT -timeout=10 porttest.dns-oarc.net.
```

結果として「POOR」または「GOOD」と表示された場合、自組織の DNS キャッシュサーバは、A.について不十分であり、DNS サーバにパッチ適用や設定変更が必要です。
「GREAT」と表示された場合、A.の点に関しては問題ありません。

3.2 自組織の DNS キャッシュサーバに対して B.を確認する

DNS 問い合わせにおいて、ID が十分にランダム化されていない場合、被害を受けやすくなります。

DNS-OARC が提供するツール「txidtest.dns-oarc.net」（英語）を使用すると、自組織の DNS キャッシュサーバに対して B.を確認することができます。

txidtest.dns-oarc.net -- Check your resolver's transaction ID behavior
https://www.dns-oarc.net/oarc/services/txidtest

このツールによる確認は、OS のコマンドラインから行います。Windows の場合、下記のように nslookup コマンドを使用することで、確認が可能です。

「txidtest.dns-oarc.net」を使用した B.の確認

```
> nslookup -querytype=TXT -timeout=10 txidtest.dns-oarc.net.
```

[5] DNS Operations, Analysis, and Research Center (DNS-OARC)。https://www.dns-oarc.net/

結果として「POOR」または「GOOD」と表示された場合、自組織の DNS キャッシュサーバは B.について不十分であり、DNS サーバにパッチ適用や設定変更が必要です。

「GREAT」と表示された場合、B.の点に関しては問題ありません。

3.3 自組織が使用している DNS コンテンツサーバに対して C.を確認する

本来、DNS サーバ（DNS コンテンツサーバ）は再帰的な DNS 問い合わせに回答するべきではありません。DNS キャッシュサーバと共用している場合でも、再帰的な DNS 問い合わせには、自組織内からのものに限定して回答するべきです。

IANA[6]が提供するツール「Cross-Pollination Scan」（英語）を使用すれば、自組織が使用している DNS コンテンツサーバが、外部からの再帰的な DNS 問い合わせに対して回答するかどうかを確認できます。下記 URL を開き、自組織が管理するドメイン名を入力してクエリ送信ボタンをクリックすると、結果が表示されます。

IANA — Cross-Pollination Scan
http://recursive.iana.org/

結果として「Vulnerable.」と表示された場合、自組織が使用している DNS コンテンツサーバは、外部からの再帰的な DNS 問い合わせに回答する状態にあります。結果の「Name Server」で表示される DNS コンテンツサーバに脆弱性の可能性があり、DNS キャッシュサーバと共用している場合、DNS サーバにパッチ適用や設定変更が必要です。

「Safe.」と表示された場合、自組織が使用しているコンテンツサーバは、外部からの再帰的な DNS 問い合わせに回答しないため、C.の点に関しては問題ありません。

4.脆弱性の影響を受けるシステムと対策方法

4.1 影響を受けるシステム

次の URL の脆弱性対策情報データベース「複数の DNS 実装にキャッシュポイズニングの脆弱性」の「影響を受けるシステム」を参照ください。

http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001495.html

4.2 脆弱性の対策方法

次の URL の緊急対策情報「複数の DNS 製品の脆弱性について」の「対策」を参照し、パッチの適用および設定変更を行ってください。

http://www.ipa.go.jp/security/ciadr/vul/20080724-dns.html

■ 本件に関するお問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター 山岸／渡辺
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
独立行政法人 情報処理推進機構 戦略企画部広報グループ 横山／大海
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

[6] Internet Assigned Numbers Authority (IANA)。http://www.iana.org/