平成 20 年 7 月 28 日

情報システム（サーバ等）管理者各位

CIO（情報化統括責任者）　菅沼　龍夫

DNS におけるキャッシュポイズニング※の脆弱性について（注意喚起）

2008 年 7 月 24 日に DNS の脆弱性を狙った攻撃ツールが公開され、現在、DNS を利用しているサーバ等の情報システムにおいて、キャッシュポイズニングの脆弱性が大きな問題となっています。

JPCERT/CC Alert 2008-07-24（http://www.jpcert.or.jp/at/2008/at080014.txt）によりますと、DNS プロトコルと複数の DNS サーバ製品にはキャッシュポイズニング攻撃を許す脆弱性があることが指摘されており、この脆弱性が使用された場合、遠隔の第三者によって DNS キャッシュサーバが偽の DNS 情報で汚染される可能性があるとのことです。

この脆弱性は複数の DNS サーバ製品に影響を及ぼします。 影響を受ける主要な製品は以下の通りです。

ISC BIND（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、その他

※DNS cache poisoning(DNS キャッシュポイズニング）とは、 DNS サーバの脆弱性を利用して偽の情報を DNS サーバへ記憶させ、その DNS サーバを使用するユーザーに対して影響を与える攻撃です。影響は攻撃者によってさまざまですが、たとえばホスト名と IP アドレスの対応を本来の情報とは違うものにして、特定のサイトへ到達できなくしたり、攻撃者がコントロールする別のサイトへ誘導したりするものがあります。なかでも、 DNS cache poisoning の攻撃を受け汚染されたサーバを利用しているユーザーが、本来意図しない金融機関や商取引のデザインに似せた虚偽のサイトに誘導され、ユーザー名やパスワードを奪われる手法が認識されており、この手法を pharming(ファーミング)と呼びます。DNS cache poisoning の攻撃手法は、DNS サーバソフトウェアの脆弱性を利用するものが古くから知られていましたが、最近では、DNS パケット中の ID を予測し応答を置き換える手法、特に TTL の短いリソースレコードに対しては比較的容易に置き換えられることが注目されています。（JPNIC News & Views vol.430 より）

したがいまして、UnixやLinux等で利用している ISC BIND（BIND 8 を含む）、 Microsoft 製 DNS サーバやネットワーク機器類において緊急な対応をお願いします。具体的な対応措置を以下に示します。

【ISC BIND】
以下のサイトより BIND-9.5.0-P1,BIND-9.4.2-P1,BIND-9.3.5-P1 のいずれかをダウンロードしてインストールして下さい。
ダウンロード：http://www.isc.org/products/BIND/

【Microsoft 製 DNS サーバ】
以下のサイトより修正プログラムをダウンロードしてインストールして下さい。なお、修正プログラム適用後、サーバの再起動が必要となります。
ダウンロード：http://www.microsoft.com/japan/technet/security/bulletin/ms08-037.mspx

この件についてのご質問は、情報支援センター情報基盤・システム運用部門（内線：7818、E-MAIL:iis@cc.miyazaki-u.ac.jp）までお問い合わせ下さい。