NTTデータ・セキュリティ株式会社

TNS Listener の脆弱性(CVE-2009-0991)に関する検証レポート

2009/4/23
NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

Oracle Database が利用する TNS Listener（クライアントからの要求を受け付けて、接続を確立させるサービス）に脆弱性が存在することが発見されました。
この脆弱性により、リモートから、TNS Listener を停止され、Oracle Database への接続不能を引き起こされる可能性があります。

今回、TNS Listener の脆弱性（CVE-2009-0991）の再現性について検証を行いました。

【影響を受けるとされているシステム】

以下のバージョンの Oracle Database が利用する TNS Listener

- 9.2.0.8
- 9.2.0.8DV
- 10.1.0.5
- 10.2.0.4
- 11.1.0.7

参考： http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html

【対策案】

Oracle 社から、修正パッチがリリースされております。
充分な検証の後、運用に支障をきたさないことをご確認の上、最新バージョンへのアップデートを行うことが推奨されます。

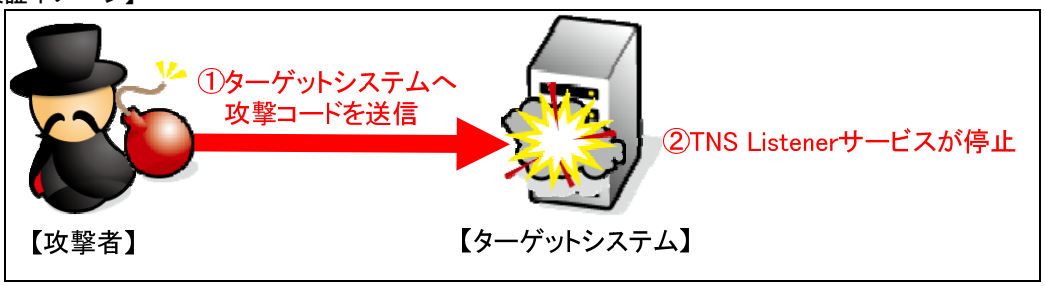
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html

【参考サイト】

CVE-2009-0991

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0991

【検証イメージ】



【検証ターゲットシステム】

Windows Server 2003 Standard Edition SP2
Oracle DataBase 10.2.0.1.0
TNS Listener 10.2.0.1.0

【検証概要】

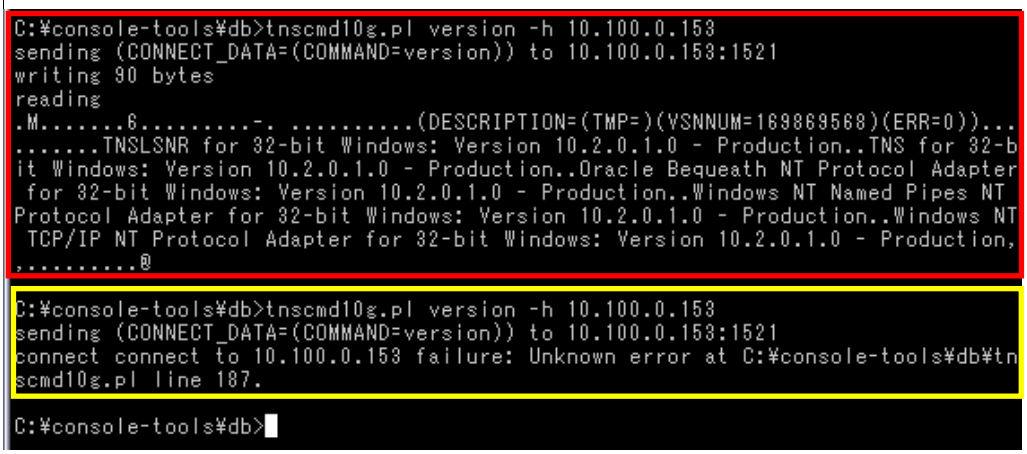
ターゲットシステムに、攻撃コードを実行することでサービス停止させます。

【検証結果】

下図の赤線で囲まれている部分は、攻撃コード送信前のターゲットシステムの TNS Listener にバージョン情報を問い合わせた画面を示しています。問い合わせに対してバージョン情報を応答していることから正常に稼動していることが確認できます。

黄色線で囲まれている部分は、攻撃コード送信後のターゲットシステムの TNS Listener にバージョン情報を問い合わせた画面を示しています。問い合わせに対して応答していないことから、サービスの停止に成功したと言えます。

ターゲットシステムの TNS Listener の停止に成功した画面



下図は、攻撃コード送信後のターゲットシステムのイベントログを示しています。これにより、TNS Listener でエラーが発生し、サービスの停止に成功したと判断できます。

ターゲットシステムのイベントログ

NTTデータ・セキュリティ株式会社

【対策案】

Oracle 社から、修正パッチがリリースされております。
充分な検証の後、運用に支障をきたさないことをご確認の上、最新バージョンへのアップデートを行うことが推奨されます。

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html

【参考サイト】

CVE-2009-0991

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0991

＊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/