NTTデータ･セキュリティ株式会社

Solaris の telnet デーモン 認証回避の脆弱性に関するレポート

2007/02/15
NTT データ･セキュリティ株式会社
辻 伸弘

【概要】

Solaris の telnet デーモンにおいて、認証の際に受け渡す情報のチェックが不適切であるため、細工した情報を送信することで悪意のあるユーザが認証を回避することが可能な脆弱性が発見されました。これにより、デフォルトの状態の Solaris に対し、非 root ユーザで認証を回避し、リモートからシステム内に侵入することが可能となります。
（明示的にシステム内で root ユーザのログインを許可している場合は、root ユーザでのログインを行うことが可能です。）
想定される被害としては、ユーザ権限での情報の取得、改ざん、または、侵入後の特権昇格による、システムの乗っ取りが考えられます。

今回、この脆弱性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】

Solaris 10(SunOS 5.10)

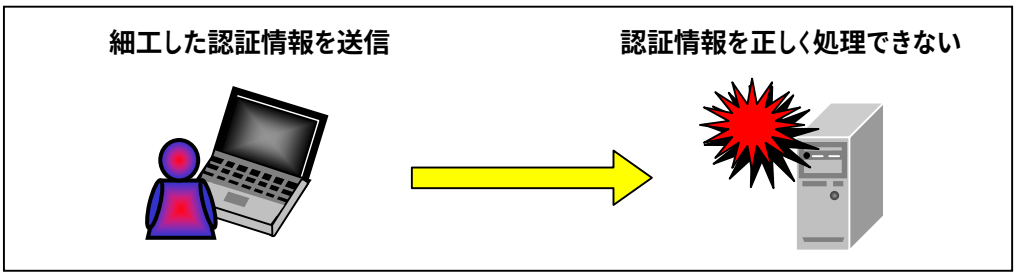
【検証ターゲットシステム】

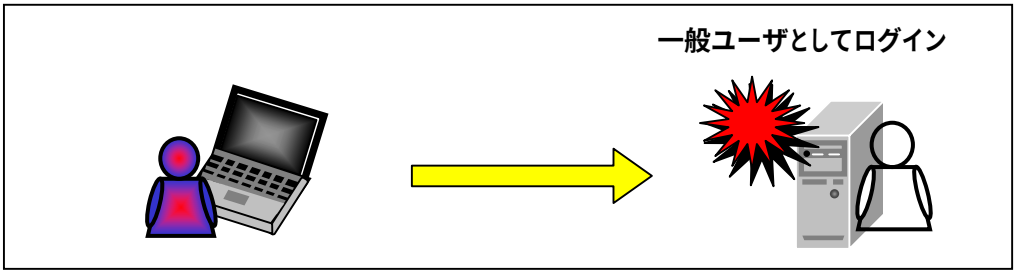
Solaris 10(SunOS 5.10)

【検証概要】

デフォルトインストールの Solaris 10 の telnet デーモンに対して、細工された認証情報を送信し、ID、パスワードによる認証を行うことなく「bin」ユーザでログインします。

【検証イメージ】





NTTデータ･セキュリティ株式会社

【検証結果】

下図の示すように、細工した認証情報を送信すると認証フェーズなしに（ログインプロンプト:ログイン ID、パスワードの入力を即す画面）ユーザ権限（bin）でログインすることに成功しました。

認証を行わずログインに成功

```
[root@localhost ~]# telnet [redacted] 10.0.0.190
Trying 10.0.0.190...
Connected to 10.0.0.190 (10.0.0.190).
Escape character is '^]'.
Last login: Tue Feb 13 21:05:58 from 10.0.0.117
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
$ id
uid=2(bin) gid=2(bin)
$
```

【対策案】

このレポート作成現在（2007 年 2 月 13 日）、ベンダーより修正プログラムはリリースされておりません。
telnet デーモンを有効にしている場合は、停止、または SSH などの代替のデーモンへと変更することを推奨いたします。
なんらかの理由から、上記、対策を講じることができない場合、telnet デーモンへは信頼できるホストからのアクセスのみを許可するといった、通信上の制御を行っていただくことを推奨いたします。

2007 年 2 月 14 日追記：
サン・マイクロシステムズ株式会社より修正プログラムがリリースされています。
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102802-1
充分な検証後、問題が発生しないことを確認し、適用を行ってください。

【参考サイト】

US-CERT
http://www.kb.cert.org/vuls/id/881872

SANS Internet Storm Center
http://isc.sans.org/diary.html?storyid=2220

＊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/