NTTデータ・セキュリティ株式会社

FreeBSD の rtld の脆弱性に関する検証レポート

2009/12/4

NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

FreeBSD の Run-Time Link Editor(以下 rtld)に脆弱性が存在することが発見されました。
rtld とは、動的にリンクされたプログラムやライブラリをロードし、間接的にプログラムを実行するために利用されます。動的リンクに利用する環境変数の処理が適切に行われないことにより、今回の問題が発生します。

この脆弱性により、ローカル環境において、一般ユーザに rtld の脆弱性を利用した攻撃コードを実行され、管理者権限を奪取される恐れがあります。
想定される被害としては、管理者権限での情報取得、改ざんが考えられます。

今回、この rtld 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】

FreeBSD 8.0、7.2、7.1、7.0

【対策案】

FreeBSD から修正プログラムがリリースされています。
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、修正プログラムの適用を行うことが推奨されます。

FreeBSD-SA-09:16.rtld
http://security.freebsd.org/advisories/FreeBSD-SA-09:16.rtld.asc

本脆弱性はシステムに一般ユーザでログインできることが前提条件となります。そのため、今一度、脆弱なパスワードが設定されているリモートログイン可能なユーザがシステム上に存在しないか確認し、存在する場合は、強固なパスワードに変更することが推奨されます。また、不要なユーザが存在する場合には直ちに削除するといった回避策を講じることが推奨されます。
ただし、正規のログインユーザによる攻撃、つまり、内部犯行を行われた場合には、上記対策は回避策とはなりません。そのため、根本的対策であるバージョンアップを講じるスケジュールを明確にすることが推奨されます。

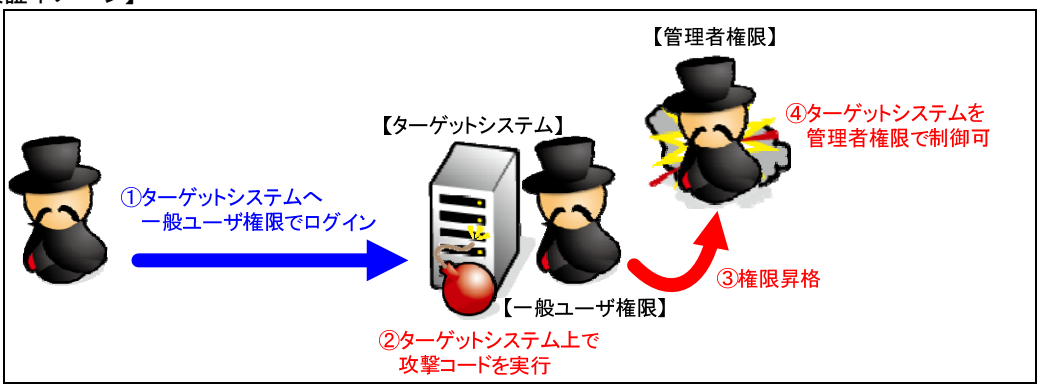
【参考サイト】

CVE-2009-4146
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4146

CVE-2009-4147
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4147

NTTデータ・セキュリティ株式会社

【検証イメージ】



【検証ターゲットシステム】
FreeBSD 7.0-RELEASE

【検証概要】
ターゲットシステムに一般ユーザでログインし、rtld の脆弱性を利用した攻撃コードを実行することで、権限昇格させます。
これにより、ターゲットシステムを管理者権限で操作可能となります。

※本脆弱性は、ターゲットシステムに一般ユーザでログインできることが前提条件です。

【検証結果】
下図の赤線で囲まれている部分は、ターゲットコンピュータに一般ユーザでログインしている情報を表しています。黄色線で囲まれている部分は、攻撃コード実行後、ターゲットシステムにおいて、管理者権限「euid=0(root)」に昇格している情報を表しています。これにより、管理者権限でのコマンド実行が可能となり、管理者権限の奪取に成功したと言えます。

ターゲットシステムの管理者権限の奪取に成功した画面

```
$
$ id
uid=1001(test) gid=1001(test) groups=1001(test),0(wheel)
$
$ sh w00t.sh
env env.c program.c program.o w00t.sh w00t.so.1.0 FreeBSD local r00t zeroday
by Kingcope
November 2009
env.c: In function 'main':
env.c:5: warning: incompatible implicit declaration of built-in function 'malloc'
env.c:9: warning: incompatible implicit declaration of built-in function 'strcpy'
env.c:11: warning: incompatible implicit declaration of built-in function 'execl'
/libexec/ld-elf.so.1: environment corrupt; missing value for
/libexec/ld-elf.so.1: environment corrupt; missing value for
/libexec/ld-elf.so.1: environment corrupt; missing value for
/libexec/ld-elf.so.1: environment corrupt; missing value for
/libexec/ld-elf.so.1: environment corrupt; missing value for
ALEX-ALEX
#
# id
uid=1001(test) gid=1001(test) euid=0(root) groups=1001(test),0(wheel)
#
```

＊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。

NTTデータ・セキュリティ株式会社

【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/