NTTデータ・セキュリティ株式会社

1.6.9p18 以前の Sudo の権限昇格の脆弱性に関する検証レポート

2008/11/18
NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

1.6.9p18 以前の Sudo コマンド（許可されたユーザに対して別のユーザの権限でコマンドを実行させるためのプログラム）に脆弱性が存在することが発見されました。
ローカル環境において、一般ユーザに Sudo コマンドの脆弱性を利用され、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、または、悪意あるプログラムをシステム内にインストールされることが考えられます。

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】

Sudo 1.6.9p18 以前のバージョン

【対策案】

このレポート作成現在（2008 年 11 月 18 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。

この脆弱性は、Sudo が以下の 2 つの両方を満たす場合に、設定されている一般ユーザが権限昇格の脆弱性を利用することが可能です。

① setenv を設定している場合
② 一般ユーザに、Sudo による管理者権限でのコマンド実行を許可している場合

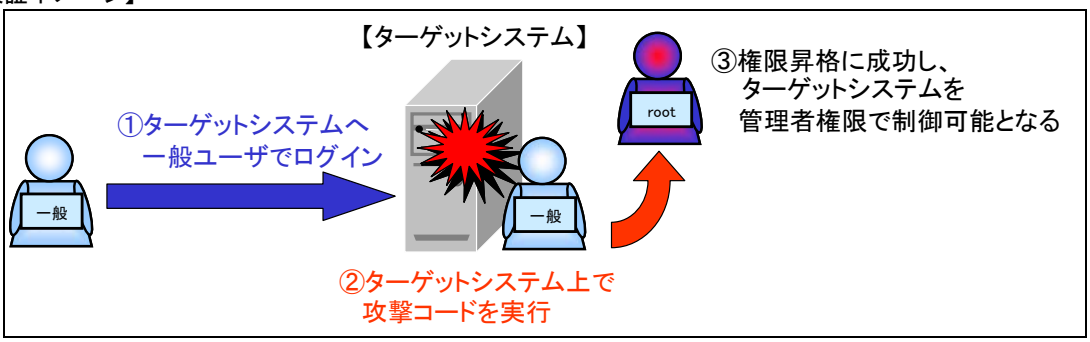
（例 1） Defaults setenv
test ALL=(root) /usr/bin/less /var/log/secure
（例 2） test ALL=(root) SETENV: /usr/bin/less /var/log/secure

＊ 上記設定では、setenv を設定し、一般ユーザ「test」にアクセス元「ALL」（すべて）から「root」権限で「/usr/bin/less /var/log/secure」コマンドを実行可能にしています。

Sudo の設定ファイル sudoers、または、visudo コマンドにて設定状況を確認し、上記設定がされているかどうか確認してください。上記設定がされている場合、その必要性の有無を確認し、不要であれば、無効にすることが暫定的な対策となります。

また、修正プログラムのリリース状況を確認し、正式な修正バージョンがリリースされた際には、速やかに最新版へアップデートすることが推奨されます。

【検証イメージ】



【検証ターゲットシステム】
Red Hat Enterprise Linux Server release 5
Sudo 1.6.9p18

【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、Sudo コマンド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、ローカルから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。
＊ この脆弱性は、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です。

【検証結果】
下図の赤線①で囲まれている部分は、ターゲットシステムに一般ユーザ「test」でログインしている情報を表しています。

赤線②の部分は、一般ユーザ「test」において、Sudo による実行が許可されているコマンドを示しています。

黄色線③の部分は、Sudo による実行が許可されているコマンドを利用し、Sudo の脆弱性を利用する攻撃コードを実行しています。

黄色線④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、管理者権限ユーザ「root」への昇格に成功している情報を表しています。

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

```
[test@localhost sudo]$ sudo -V
Sudo version 1.6.9p18
[test@localhost sudo]$
[test@localhost sudo]$ id
uid=500(test) gid=500(test) 所属グループ=500(test) context=user_u:system_r:unconfined_t ①
[test@localhost sudo]$
[test@localhost sudo]$ sudo -l
パスワード:
User test may run the following commands on this host:
    (root) /usr/bin/less /var/log/secure ②
[test@localhost sudo]$
[test@localhost sudo]$ ./sudo_exploit "/usr/bin/less /var/log/secure" ③
Sudo <= 1.6.9p18 local root exploit
CONGRATULATIONS, IT'S A ROOTSHELL!
sh-3.1#
sh-3.1# id
uid=0(root) gid=0(root) 所属グループ=500(test) context=user_u:system_r:unconfined_t ④
sh-3.1#
```

【対策案】

このレポート作成現在（2008 年 11 月 18 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。

この脆弱性は、Sudo が以下の 2 つの両方を満たす場合に、設定されている一般ユーザが権限昇格の脆弱性を利用することが可能です。

① setenv を設定している場合
② 一般ユーザに、Sudo による管理者権限でのコマンド実行を許可している場合

（例 1） Defaults setenv
test ALL=(root) /usr/bin/less /var/log/secure
（例 2） test ALL=(root) SETENV: /usr/bin/less /var/log/secure

＊ 上記設定では、setenv を設定し、一般ユーザ「test」にアクセス元「ALL」（すべて）から「root」権限で「/usr/bin/less /var/log/secure」コマンドを実行可能にしています。

Sudo の設定ファイル sudoers、または、visudo コマンドにて設定状況を確認し、上記設定がされているかどうか確認してください。上記設定がされている場合、その必要性の有無を確認し、不要であれば、無効にすることが暫定的な対策となります。

また、修正プログラムのリリース状況を確認し、正式な修正バージョンがリリースされた際には、速やかに最新版へアップデートすることが推奨されます。

【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/