NTTデータ・セキュリティ株式会社

Sambaのシンボリック処理の欠陥により任意のファイルにアクセスされる脆弱性に関する検証レポート

2010/02/12
診断ビジネス部
辻　伸弘
松田　和之

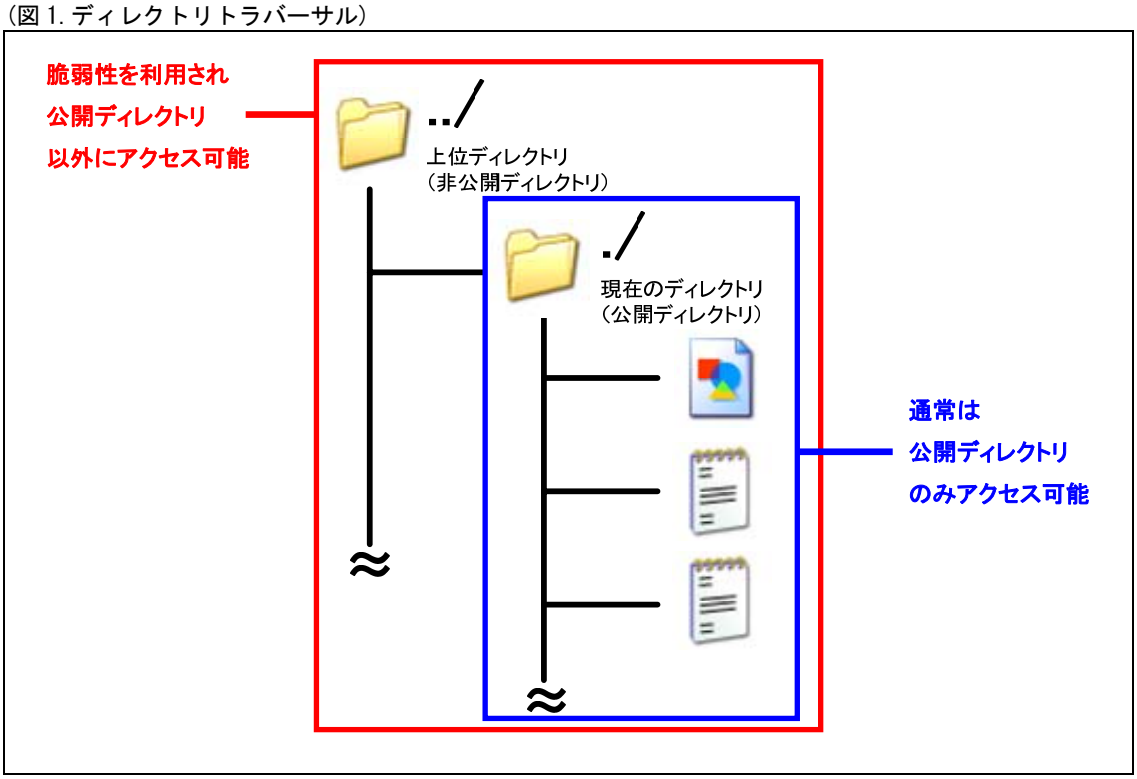
【概要】

Samba のシンボリックリンク処理に欠陥があり、ディレクトリトラバーサル攻撃を受ける脆弱性が発見されました。Samba サーバにログイン（匿名ログイン含む）が可能であり、かつ、書き込み可能である場合、細工したシンボリックリンクを作成されることにより、ターゲットシステムの任意のローカルファイルを閲覧される危険性があります。

ディレクトリトラバーサル攻撃とは、相対パス（現在位置を基点として目的位置までのパスを記述する記述方法）を利用して、Samba サーバ上で公開している以外の、管理者が意図しないディレクトリ、及び、ファイルにアクセスする攻撃手法です。

通常、Samba サーバでは、設定されている公開ディレクトリ以外にアクセスを行うことはできません。（図 1. 青枠部分）
しかし、ディレクトリトラバーサルの脆弱性を利用することで、システム内の重要情報を含むファイルやディレクトリが存在する非公開のディレクトリやファイル（図 1. 赤枠部分）へのアクセスが可能となります。
脆弱性を利用し、本来アクセス不可能なディレクトリへと横断（トラバーサル:traversal）、アクセスすることからディレクトリトラバーサルと呼ばれています。

（図 1. ディレクトリトラバーサル）



想定される被害としては、悪意のあるユーザにより、Samba サーバ上で公開しているファイル以外のシステムの固有情報を含むファイル等が漏洩することが挙げられます。

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】
Samba 3.4.5

【対策案】
このレポート作成現在（2010 年 2 月 12 日）、修正プログラムはリリースされておりません。

そのため、暫定対処として、Samba サーバの設定ファイル（smb.conf）の[global]セクションにおいて、以下の設定を追加することが推奨されます。設定後、Samba サーバを再起動することで設定が有効になります。

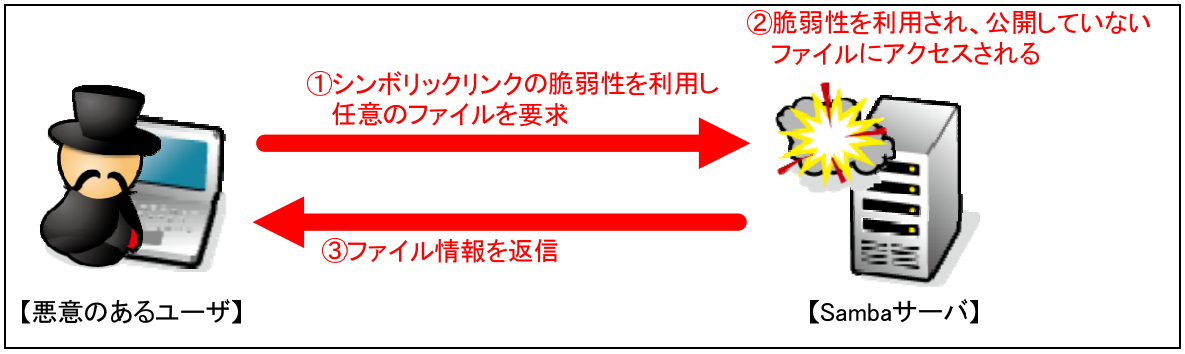
```
wide links = no
```

これにより、公開ディレクトリ以外へのリンクを防ぐことができます。

本脆弱性は、Samba サーバにログイン（匿名ログイン含む）が可能であり、かつ、書き込み可能であ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、修正プログラムがリリースされ次第、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】
[Samba] Claimed Zero Day exploit in Samba
http://www.samba.org/samba/news/symlink_attack.html

【検証イメージ】



【検証ターゲットシステム】
Samba 3.4.5

【検証概要】
ターゲットシステムの Samba サーバにログインし、シンボリックリンクの脆弱性を利用した攻撃コードを実行することで、ディレクトリトラバーサル攻撃を行います。
これにより、ターゲットシステム内の任意のファイルの閲覧が可能となります。

※本脆弱性は、ターゲットシステムの Samba にログインできることが前提条件です。

NTTデータ・セキュリティ株式会社

【検証結果】

下図は、ディレクトリトラバーサルの脆弱性を利用し、ターゲットシステムのユーザ情報が格納されている「/etc/passwd」ファイルを、Samba クライアントから読み出した画面です。
赤枠（赤枠内の「：」（コロン）より前の部分）で示すとおり、ターゲットシステムに存在するユーザの一覧を取得できたと言えます。これにより、悪意のあるユーザに、SSH 等から当該ユーザに対するオンラインクラックを行われ、システムへの更なる制御の奪取を許す危険性があります。

ターゲットシステムの/etc/passwd を読み出した画面

```
smb: ¥foobar¥> more etc/passwd
getting file ¥foobar¥etc/passwd of size 2507 as /tmp/smbmore.pZ1avt (188.3 KiloBytes/sec)
(average 188.3 KiloBytes/sec)
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
```

*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/