

Analysis of the ATD OpenSSL Mass Exploiter

分類 ELF Binary dtors section rewrite
 ツール属性 GZIP 圧縮ファイル
 再現性 リモート

技術解説

概要

OpenSSL 0.9.6d 以前に含まれるバッファオーバーフローを利用した攻撃ツール。アーカイブの中には、mass、vuln、openssl-too、osslmass2 の4種類のファイルがまとめられている。これら4つのファイルは Linux.RST.B ウィルスとして検出される。

影響

検証した攻撃ツールは、OpenSSL の脆弱性を利用して Apache (通常は Apache か nobody) ユーザ権限を取得するためのプログラムをまとめた圧縮ファイルである。

アーカイブには4つのツールがあり、そのうちの1つのツールを使うことで、脆弱な OpenSSL が動作しているサーバの apache ユーザ権限を奪える可能性がある。また、Linux 実行形式(ELF)ファイルを改ざんする機能を持つ。

影響を受けるOS、サービス

影響 ○:脆弱性あり、×:脆弱性なし

(2002/7/30現在)

OS	サービス	バージョン	影響	備考
Linux 全般	OpenSSL	0.9.6d以前	○	<ul style="list-style-type: none"> Linux 実行形式ファイル(ELF)が動作するカーネルバージョンであること。 ターゲットホストで OpenSSL 0.9.6d 以前のバージョンが稼動していること。

参考 URL:

CERT Advisory:

<http://www.cert.org/advisories/CA-2002-23.html>

LURHQ:

<http://www.lurhq.com/atd.html>

対策方法

1)対策

ウィルス対策ソフトを導入し、ベンダーが提供する最新版のウィルス定義ファイルに更新しておくことで検知することが可能である。また、OpenSSL 0.9.6d 以前が稼動しているホストでは、問題が対策済みである OpenSSL0.9.6e 以降のバージョンにアップデートする。

OpenSSL 最新バージョン入手先 URL:
<http://www.openssl.org/source/>

2) Advisory情報

CERT Advisory:

<http://www.cert.org/advisories/CA-2002-23.html>

LURHQ:

<http://www.lurhq.com/atd.html>

3) Virus情報

Symantec:

<http://securityresponse.symantec.com/avcenter/venc/dyn/10739.html>

SOPHOS:

<http://www.sophos.com/virusinfo/analyses/linuxrstb.html>

検証有無

結果 ○:成功、×:失敗、-:未検証

(*1)Apacheユーザ権限の取得失敗

OS	サービス	バージョン	結果
RedHat Linux 7.3 (J)	mod_ssl/2.8.7 OpenSSL	0.9.6b	× (*1)
上記以外の組み合わせ			-

検証結果

1) 検証環境

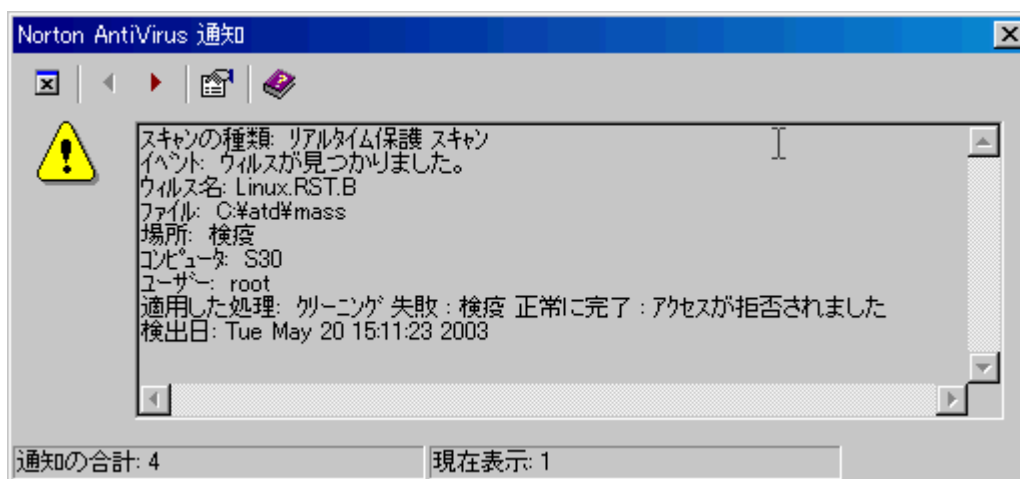
	OS	サービス	備考	IP Address
サポートホスト	Windows 2000 Professional (J)	-	Norton Anti Virus、vigil、nmap	192.168.1.2
攻撃側ホスト	RedHat Linux 7.3 (J)	-	chkrootkit、tripwire	192.168.1.1
ターゲットホスト	RedHat Linux 7.3 (J)	OpenSSL 0.9.6b	Apache/1.3.23 mod_ssl/2.8.7 OpenSSL/0.9.6b	192.168.1.1

2) 検証結果

ツールを実行したが、apache の実行権限が取れなかった。

<ウィルスチェックの結果>

atd.tgz に含まれる全てのファイルが Linux.RST.B として検知された。



<Strings のログ>

ログからは既存ファイルへの書き込みを確認できなかった。

<Strace のログ>

ログからは既存ファイルへの書き込みを確認できなかった。

<ポートの確認>

ツール実行後に開いたポートは確認できなかった。

<ログの整合性検査>

chkrootkit のログからログが修正された痕跡は確認できなかった。

<システムファイルの整合性検査>

tripwire のログからカレントディレクトリ、および /bin 以下の Linux 実行形式ファイル(ELF)が修正されたことが確認できた。

<ハッシュ値の検査>

tripwire を使った調査の結果から、修正が確認されたファイルのハッシュ値を比

較した結果、いくつかのファイルのハッシュ値が変更されていることを確認できた。

<パケットダンプ>

各ツールが流すパケットをダンプした結果、openssl-too が外部ホストに通信を試みていることを確認できた。

<改ざんされたファイルの動作確認>

改ざんされたプログラムの動作を確認した結果、動作そのものに問題は確認できなかった。しかし、安全な Strace コマンドで改ざんされたプログラムの動作を確認した結果、ハッシュ値が変わったファイルに関して、子プロセスを生成するようになっていることが確認できた。以下は、df コマンドの、ハッシュ値変更前の strace 結果と、ハッシュ値変更後の strace 結果を比較したものである。

```
$ diff dfbefore.txt dfafter.txt
20c20,21
< getpid()                = 1027
---
> getpid()                = 1032
> fork()                  = 1033                // 追加されている //
26c27,28
< mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40018000
---
> mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40
> 018000
194c196
< statfs("/home", {f_type="EXT2_SUPER_MAGIC", f_bsize=4096, f_blocks=3884340, f_bfree=383
f_files=1974720, f_ffree=1968593, f_namelen=255}) = 0
---
> statfs("/home", {f_type="EXT2_SUPER_MAGIC", f_bsize=4096, f_blocks=3884340, f_bfree=383
f_files=1974720, f_ffree=1968593, f_namelen=255}) = 0
207c209
< write(1, "/dev/hda6          15537360 "..., 62/dev/hda6          15537360    210
14537112    2% /home) = 62
---
> write(1, "/dev/hda6          15537360 "..., 62/dev/hda6          15537360    210
14537108    2% /home) = 62
```

<プロセスの確認>

ツールを使う前のプロセスと、使った後に安全な ps コマンドで出力したプロセスの状態を比較した結果、新たに作成されたプロセスを確認することはできなかった。

痕跡

1) ログ

ターゲットホストの Apache が出力する accept.log に以下のエラーが出力された。

```
192.168.1.100 - - [06/May/2003:15:00:38 +0900] "GET /sumthin HTTP/1.0" 404 267 "-" "-"
```

2) 痕跡

mass、mass.log(massのログファイル)、vuln、openssl- too、osslmass2 が残る。