

## ウィルス解析報告書

ウイルス名	Trojan.Linux.JBellz
プログラム名及び容量 (添付ファイル名)	不定 2,888バイト (拡張子.mp3のファイル)
種別	トロイの木馬(バッファオーバーフロー攻撃型)
プログラム言語:	gccおよびアセンブラ
発症環境	SuSE Linux 8.0 または Slackware Linux 8.0 上で mpg123 MPEGオーディオプレイヤー (の特定のバージョン) を利用している環境
発見日時	2003年1月14日
発見場所 (発信地)	不詳
危険性	きわめて低い(5段階中1以下。対象となる環境が非常に限られたものであるため)
発症条件	SuSE Linux 8.0 または Slackware Linux 8.0 上で mpg123 MPEGオーディオプレイヤー デベロッパーバージョン0.59sを利用して該当トロージャンファイルを演奏したとき
ウイルスの活動、影響	<p>このウイルスは、実際にはトロイの木馬であり、感染力を持たない。</p> <p>MP3ファイルにトロイの木馬が仕掛けられるケースはこれが初めてのため、大きなニュースとなったが、実際にはバッファオーバーフロー脆弱性のあるアプリケーションであれば、それがどのようなアプリケーションであれ、原理的にはトロイの木馬は作成可能といえる。</p> <p>このトロイの木馬が攻撃対象としているのはmpg123 MPEGオーディオプレイヤーソフトウェア (<a href="http://www.mpg123.de">http://www.mpg123.de</a>)である。 このバージョンPre0.59sにおいて、MAX_INPUT_FRAMESIZEのサイズが固定値かつ不当に小さい値であったため、意図的に変造されたMP3ファイルによってバッファオーバーフローが発生する弱点があった。</p> <p>Trojan.Linux.JBellzはこのバッファオーバーフロー脆弱性を利用して自身のコードを実行させるものである。</p> <p>トロイの木馬である、このMP3ファイルが演奏されると、コンソールに</p> <pre>rm -rf in 5 seconds.. CTRL-c to abort</pre> <p>が表示され、さらに</p> <pre>pP</pre> <p>が表示される。この表示は1秒ごとに1個ずつ増えていき、最後には</p> <pre>pPpPpPpPpP</pre> <p>となる。放置しておくとも/home以下のユーザーホームディレクトリがrmコマンドによって削除される。</p>
被害の規模	2003年1月15日時点では確認されていない
亜種、変種の有無	確認されていない
ウイルス動作概要	<p>トロイの木馬として作成されたMP3ファイルをmpg123 MPEGオーディオプレイヤーで再生すると、バッファオーバーフローが発生してトロイの木馬内部のプログラムコードが実行される。</p> <p>はじめにシステムコールを呼び出して、標準エラー出力に</p> <pre>rm -rf in 5 seconds.. CTRL-c to abort</pre> <p>を出力する。</p> <p>その後、標準エラー出力に「pP」と出力して1秒間停止する。これを5回繰り返す。</p>

	最後に  /bin/sh -c rm -rf  を実行してプログラムを強制終了する。 これによりユーザーホームディレクトリ(/home/<user name>)が削除される。
感染・発症防止方法	mpg123プレイヤーを利用している場合は、セキュリティホール対策がなされたバージョンにアップデートする。
ウイルスの駆除方法	<確認> ファイルサイズが2,888バイトのMP3ファイルはこのトロイの木馬である危険がある。 通常のMP3ファイルは1分あたり1Mバイト程度の容量を持ち、これほど小さいファイルは壊れているかトロイの木馬である可能性が高い。  <駆除> 該当のMP3ファイルを削除する。
その他	報告書作成 : 2003年1月18日現在

## Trojan.Linux.Jbellz フローチャート

