セキュリティ・ネットワーク学実験 3(B2)
アプリケーション脆弱性実習レポート

2600200087-2
Oku Wakana
奥 若菜

Jun.29 2022

1　問 1 アーカイブソフトの異常終了 (1)

1.1　スタック領域におけるバッファオーバーフロー

外部からの入力によって確保したバッファ以上のデータがプログラムに読み込まれ、それが変数にコピーされることで、コピー先のバッファからデータが溢れ、隣の変数の内容が上書きされてしまうことがある。このような現象をバッファオーバーフローという。ここでは、脆弱アーカイブソフトに含まれるスタック領域におけるバッファオーバーフローの脆弱性を確認する。

1.2　演習 1/9

脆弱アーカイブソフトを使って ArchiverSample.zip を展開し、その様子をキャプチャした。図 1 のようにファイルを展開したところ、動作が完了し、図 2 のように sample.txt という名前のファイルが作成された。

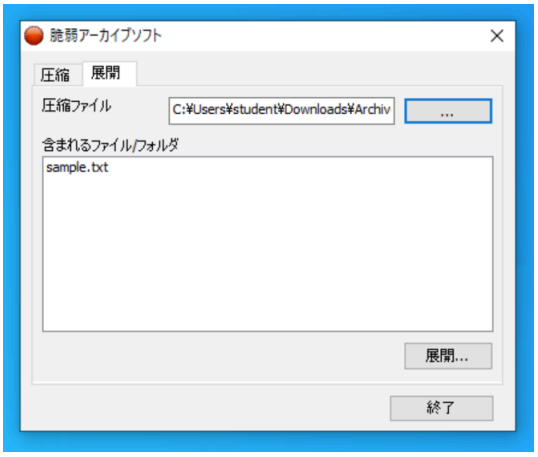

図 1　ファイル展開

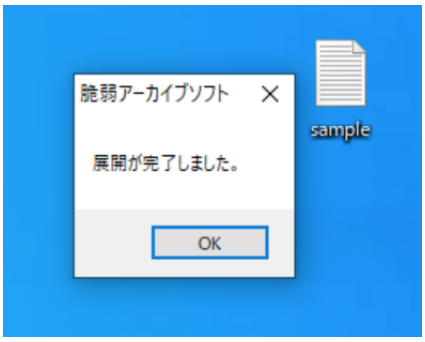

図 2　展開完了

1.3　演習 3/9

脆弱アーカイブソフトを使って ArchiverCheckBOF.zip を展開し、その様子をキャプチャした。図 2 のようにファイルを展開しようとしたところ、図 4 のように、脆弱アーカイブソフトが異常終了し、zip ファイルを展開することはできなかった。これは、zip ファイルに含まれるファイルまたはフォルダ名が、あらかじめ確保したバッファ以上の長さだったため、バッファオーバーフローが起きたことよって、異常終了したと考えられる。

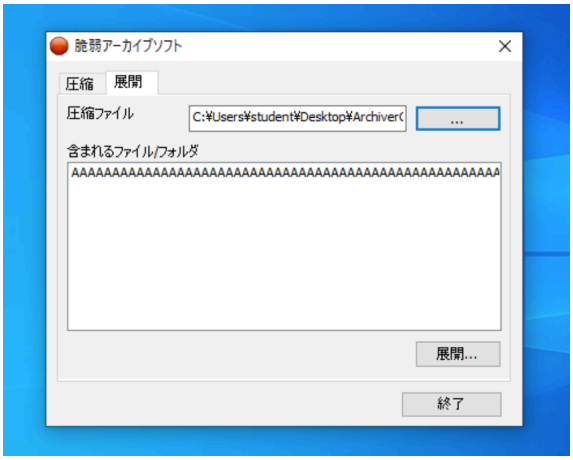

図 3　ファイル展開

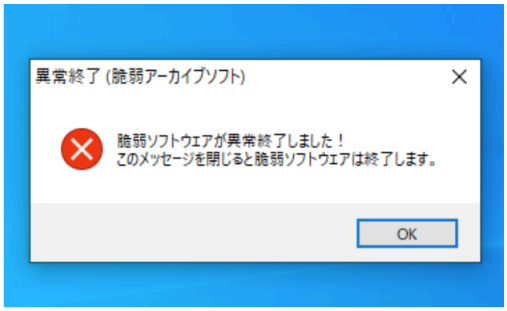

図 4　異常終了

2　問 2 アーカイブソフトの異常終了 (2)

2.1　演習 4/9

脆弱アーカイブソフトを使って、擬似攻撃ファイル ArchiverAttackBOF.zip を展開し、その様子をキャプチャした。脆弱性が悪用されることにより、ダイアログを表示させるマシンコードが実行された結果、下の図 5 のようなダイアログが表示された。演習 3/9 との違いとして、プログラムが異常終了した結果、ダイアログが表示されたのではなく、マシンコードによって表示されたものであるという点が挙げられる。

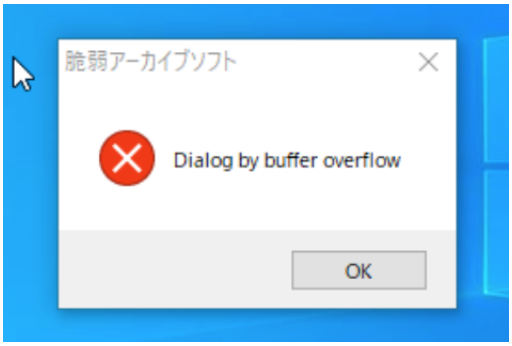

図 5　実行結果

2.2　問 2.1

バッファオーバーフローが起きた際に、プログラムが異常終了する理由は、UNIX 系の OS 上では、不正なメモリにアクセスするプロセスは SIGSEG シグナルを受けとるためである。これにより、プロセスが OS によって止められ、異常終了したと考えられる。また、他の OS を利用する場合も同様に例外を受け取る。プログラムの表示がおかしくなったり、変数値がおかしくなったりする理由としては、バッファオーバーフローによって、溢れたデータで他のメモリ内容が上書きされ、変数の値が書き換えられるためと考えられる。

2.3　問 2.2

攻撃者によって、任意のプログラムが送り込まれる方法と、そのプログラムが実行される原理を説明する。攻撃者は、スタックオーバーフローを用いて、任意のマシンコードをメモリ上に書き込む。そして関数の return アドレスを、そのマシンコードが書かれた先頭アドレスに書き換えることで、任意のプログラムを実行させる。

2.4　問 2.3

フォーマット文字列を用いた攻撃では、フォーマット文字列として %n が最も危険だといわれている。この %n を用いた攻撃の原理を説明する。%n は、これまでの書式編集出力で何バイトのデータが書き出されたかの値を整数変数に書き戻すことを指示する書式である。これを使い、ポインタ変数の値を任意のアドレスに書き換えることで、実行したいマシンコードの先頭アドレスに飛ばすことができる。

3　問 3 脆弱 Archiver の修正

1,2 章で確認した脆弱性を、ソースコードを修正することで、異常終了が起こらないようにする。脆弱性の原因は、圧縮されたファイル内のファイル名のコピーに、strcpy 関数を使っているためだと考えられる。これを strncpy 関数に置き換え、コピーする文字列の長さを制限することで、バッファオーバーフローが起こることを防ぐ。

下の図 6 は、修正をおこなった後に ArchiverCheckBOF.zip を展開した結果である。異常終了することは無くなったが、別のエラーが発生し、ファイルを作成することはできなかった。

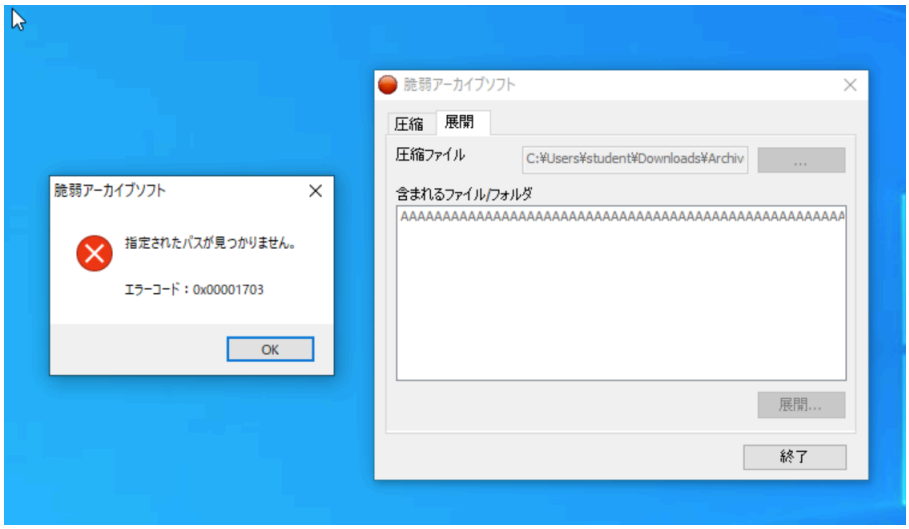

図 6　実行結果

4　問 4 整数オーバーフロー

4.1　演習 3/7

脆弱アーカイブソフトを使って、ArchiverCheckIOF.zip を展開したところ、整数オーバーフロー脆弱性がバッファオーバーフローを誘発し、下の図 7 のようにプログラムが異常終了した。

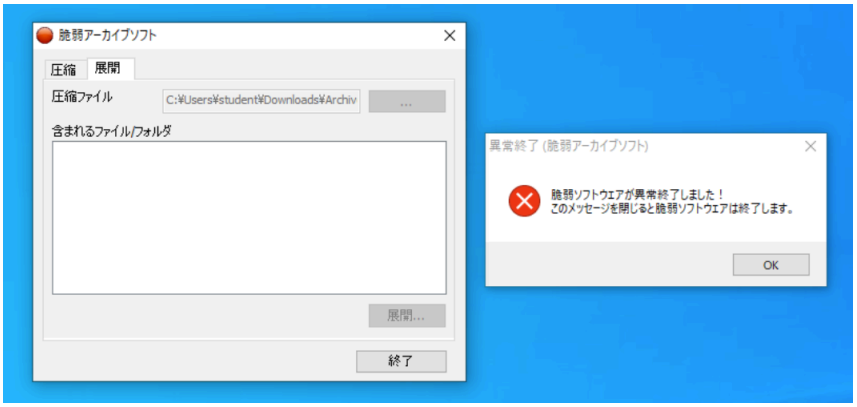

図 7　実行結果

4.2　演習 4/7

脆弱アーカイブソフトを使って、擬似攻撃ファイル ArchiverAttackIOF.zip を展開し、その様子をキャプチャした。整数オーバーフロー脆弱性が悪用されることにより、バッファオーバーフローが誘発され、ダイアログを表示させるマシンコードが実行された結果、下の図 8 のようなダイアログが表示された。演習 3/7 との違いとして、プログラムが異常終了した結果、ダイアログが表示されたのではなく、マシンコードによって表示されたものであるという点が挙げられる。

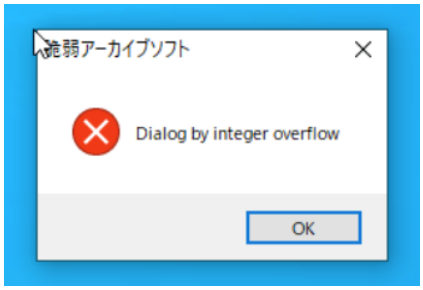

図 8　実行結果