平成30年度 春期 情報処理安全確保支援士

＜午後Ⅰ解答・解説＞

＜問1＞　ソフトウェアの脆弱性

■設問1

[試験センターによる解答例]

a：カ
b：ウ

a：解答群の中で，確保済みメモリ領域を超えてデータを書き込んでしまうことで任意の攻撃コードが実行され得る脆弱性は「バッファオーバフロー」である。

b：解答群の中で，解放したメモリ領域を後から使用してしまう脆弱性に該当するのは「Use-After-Free」である。

■設問2

[試験センターによる解答例]

785634120a（10字）

問題文にあるように，図3の(1)でCreateNoteメンバ関数によって確保されていたNote構造体用のメモリ領域が，図3の(2)でDeleteNoteメンバ関数によって解放され，その後図3の(3)でRegisterNameメンバ関数が呼ばれた場合，char[8]用のメモリ領域が図3の(1)で確保されていた領域と同じアドレスに割り当てられる可能性がある。その場合，RegisterNameメンバ関数で読み込まれる攻撃者の入力値により，元々Note構造体用であったメモリ領域が上書きされることになる。設問は攻撃者の指定したアドレスが0x12345678，改行コードが0x0aであった場合の入力値の具体的なバイト列であるが，その前提として，アドレスは32ビット，バイトオーダがリトルエンディアンのバイトマシンによって扱われるものとしている。

攻撃者の入力値が読み込まれるのは図1の22行目のscanf関数であり，入力値の後に改行コードが続いていることが分かる。リトルエンディアンとは，複数バイトの2進数をメ

モリに配置する際に，最下位のバイトから順番に並べる方式である。したがって，アドレス 0x12345678 は 78563412 となり，これに改行コードの 0a が続くため，入力値のバイト列は 785634120a となる。なお，リトルエンディアンとは逆に，最上位のバイトから順番に並べる方式をビッグエンディアンという。

■設問 3

[試験センターによる解答例]

c：(エ)

問題文に「次に CreateNote メンバ関数が呼び出された際，攻撃コードに処理が遷移することになる」とある。図 1 の 13 行目にあるように，CreateNote メンバ関数内で使われているライブラリ関数は new であり，表 1 でこれに該当するアドレスは(エ)の 0x08049e40 である。

■設問 4

[試験センターによる解答例]

d：0x0b123400

問題文に「m_note->msg が指し示すメモリ領域に攻撃コードが書き込まれていて，その先頭アドレスが 0x0b123400 と分かっていたとする」とあるので，アドレス 0x08049e40 に書き込む値は 0x0b123400 である。

■設問 5

[試験センターによる解答例]

e：ヒープ

図 1 の 26 行目にあるように，RegisterMsg メンバ関数では，new で 100 バイトのメモリ領域を確保している。このように，new で動的に確保した場合に用いられるのはヒープ領域である。

■設問 6

[試験センターによる解答例]

ライブラリ関数はデータ実行防止の対象ではないメモリ領域に配置されているから（37 字）

データ実行防止（Data Execution Prevention：DEP）とは，指定されたメモリ領域でのコードの実行を禁止する機能であり，バッファオーバフロー攻撃の対策として有効である。しかし，ライブラリ関数は DEP の対象ではないメモリ領域に配置されているため，関数テーブルに書き込むアドレスとして共有ライブラリ内のメモリアドレスを選べば，DEP が有効化されていた場合でも，攻撃者は任意のコードを実行できる可能性がある。

■設問 7

[試験センターによる解答例]

f：（ア）

/bin/sh を起動して任意のシェルコマンドを実行するには system 関数を用いる。表 2 でこれに該当するアドレスは（ア）の 0xf7cc8da0 である。

■設問 8

[試験センターによる解答例]

g：DisplayNote

ASLR が有効化されていた場合でも共有ライブラリ内のメモリアドレスを特定するには，メモリアドレスを出力する必要がある。図 1 でこれに利用できそうなメンバ関数を探すと，

printf 関数でメモリの内容を出力している DisplayNote が該当する。

■設問 9

[試験センターによる解答例]

h：m_note = NULL;

図 1 の 37～39 行目で delete を用いて Note 構造体のメモリ領域を解放しているが，m_note を初期化していないため，元の値が残ったままになっている。これを修正するには，図 1 の 39 行目の直後に "m_note = NULL;" という 1 文を加え，m_note を初期化すればよい。

＜問 2＞ 情報セキュリティ対策の強化

■設問 1

[試験センターによる解答例]

(1) a：x1.y1.z1.4
(2) b：迷惑メール対策サーバ
c：Web メールサーバ
d：外部メールサーバ

(1) 図 2 の TXT レコードは SPF の設定であり，T 社からインターネットにメールを送信するサーバの IP アドレスを登録する。表 2 にあるように，T 社でその機能をもつサーバは外部メールサーバである。したがって [a] には"x1.y1.z1.4"が入る。

(2)

b：インターネットからのメールを最初に受信するサーバは，不審なメールや迷惑メールを破棄する機能をもつ「迷惑メール対策サーバ」である。

c：表 2 の「迷惑メール対策サーバ」の機能の概要に「受信したメールを Web メールサーバに SMTP で転送する」とあるように，[c] には「Web メールサーバ」が入る。

d：「Web メールサーバ」からのメールを受信し，インターネットに送信するサーバであるから，[d] には「外部メールサーバ」が入る。