

[UNIX] wvWare Library Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0026.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/11/04

To: list@securiteam.com

Date: 11 Jul 2004 11:36:40 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

wvWare Library Buffer Overflow Vulnerability

SUMMARY

Caol n McNamara and Dom Lachowicz's <<http://wvware.sf.net/>> wvWare is "a library used to load and parse Microsoft Word files on unix-based systems. wvWare is used in some third-party programs to view and convert Microsoft Word documents to other formats".

Caol n McNamara and Dom Lachowicz's wv library has been found to contain a buffer overflow condition that can be exploited through a specially crafted document.

DETAILS

Vulnerable Systems:

* wvWare version 0.7.4, 0.7.5, 0.7.6 and 1.0.0

The issue lies in the handling of the DateTime field of a document as can be seen from the following lines of code taken from field.c and the function wvHandleDateTimePicture():

```
..
    default:
```

Securiteam: [UNIX] wvWare Library Buffer Overflow Vulnerability

```
temp[0] = *token;
temp[1] = '\0';
strcat (timestr, temp);
break;
}
..
```

The above section of code can be reached if the wv library is presented with a token that it does not recognize. The utilization of the insecure function call `strcat()` without appropriate bounds checking leads to a classic and exploitable buffer overflow.

The following is a walkthrough of a sample exploitation of the buffer overflow that will execute the command "id > /tmp/wv_exploit" upon success.

```
$ id
uid=501(farmer) gid=501(farmer) groups=501(farmer)
```

```
$ ls /tmp/wv_exploit
ls: /tmp/wv_exploit: No such file or directory
```

```
$ dd if=wv_exploit.doc of=a3.doc ibs=1 count=42945
42945+0 records in
83+1 records out
```

```
$ perl wv_exploit.pl >> a3.doc
```

```
$ wvHtml wv_exploit.doc exploit.html
```

```
$ cat /tmp/wv_exploit
uid=501(farmer) gid=501(farmer) groups=501(farmer)
```

The final exploit document size must be a multiple of 4096 bytes to be valid. Because of some input filtering the shellcode and return address can only contain ASCII characters (00–7f) not including any of the following: 0x22, 0x60, 0x48, 0x68, 0x41, 0x61, 0x4d, 0x6d, 0x53, 0x73, 0x44, 0x64, 0x59, 0x79.

Analysis:

If an attacker can convince a user to open an exploit document in HTML mode using an application that builds upon the wv library, it is possible for the attacker to execute arbitrary code under the privileges of that user.

Workaround:

Users should be careful to open documents from only trusted sources. When opening Microsoft Word documents with applications utilizing the wv library ensure that HTML view is not enabled. Careful low-level scrutiny of the document in question can also reveal whether or not the document is valid or not.

Securiteam: [UNIX] wvWare Library Buffer Overflow Vulnerability

Vendor Status:

Dom Lachowicz has posted the following patch details:

http://www.abisource.com/bonsai/cvsview2.cgi?diff_mode=context&whitespace_mode=show&root=/cvsroot&subdi
CVS diff from 1.19 to 1.20

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0645>
CAN-2004-0645

Disclosure Timeline:

06/29/2004 Initial vendor contact

07/06/2004 Vendor response

07/09/2004 Public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<mailto:idlabs-advisories@idefense.com> iDEFENSE.

The original article can be found at:

<http://www.idefense.com/application/poi/display?id=115&type=vulnerabilities>
<http://www.idefense.com/application/poi/display?id=115&type=vulnerabilities>

=====

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.