

wvWare Library Buffer Overflow Vulnerability

IDEFENSE Security Advisory 07.09.04:

I. BACKGROUND

Caolán McNamara and Dom Lachowicz's 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.

II. DESCRIPTION

Caolán 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.

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:
            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.

III. 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.

IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in version 0.7.4, and a slight variant of this vulnerability in versions 0.7.5, 0.7.6 and 1.0.0.

V. 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.

VI. VENDOR RESPONSE

Dom Lachowicz has posted the following patch details:

```
http://www.abisource.com/bonsai/cvsview2.cgi?diff_mode=context&whitespace_mode=show&root=/cvsroot&subdir=wv&command=DIFF_FRAMESET&root=/cvsroot&file=field.c&rev1=1.19&rev2=1.20
```

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CAN-2004-0645 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

VIII. DISCLOSURE TIMELINE

06/29/2004 Initial vendor contact
07/06/2004 Vendor response
07/09/2004 Public disclosure

IX. CREDIT

Karol Wieseck is credited with discovering this vulnerability.