

[NEWS] OpenOffice and StarOffice Suites WMF and EMF Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-01/msg00009.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 7 Jan 2007 18:20:27 +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>

OpenOffice and StarOffice Suites WMF and EMF Vulnerabilities

SUMMARY

John Heasman of NGSSoftware has discovered several high risk vulnerabilities in the handling of WMF and EMF graphics formats within the OpenOffice StarOffice suite.

DETAILS

Vulnerable Systems:

- * OpenOffice versions prior to 2.1.0
- * StarOffice 6, 7 and 8

Immune Systems:

- * OpenOffice version 2.1.0 and newer

The vulnerabilities, three heap overflows, affect OpenOffice version prior to 2.1.0 and StarOffice 6, 7 and 8. If an attacker can coax a user into opening a specially crafted document then the attacker can execute arbitrary code in the security context of their victim.

Technical Details:

[NEWS] OpenOffice and StarOffice Suites WMF and EMF Vulnerabilities

1) From svtools\source\filter.vcl\wmf\winwmf.cxx

```
case W_META_ESCAPE :
..
sal_uInt32 i, nStringLen, nDXCount;
..
aMemoryStream >> aPt.X()
>> aPt.Y()
>> nStringLen;

sal_Unicode* pBuf = aString.AllocBuffer( (sal_uInt16)nStringLen );
for ( i = 0; i < nStringLen; i++ )
aMemoryStream >> pBuf[ i ];
```

nStringLen is a sal_uInt32; it is cast to a sal_uInt16 for the allocation then the original 32 bit value is used as a count to fill the buffer, thus any length greater than 0xFFFF results in a heap overflow. Code execution is possible via a function pointer overwrite or arbitrary DWORD overwrite if the user opens a malicious WMF, or a container document (such as a Microsoft Word document) in which it is embedded.

2) From svtools\source\filter.vcl\wmf\enhwmf.cxx
case EMR_POLYPOLYGON :

```
INT32 i, nPoly, nGesPoints;
..
*pWMF >> nPoly >> nGesPoints;
..
pPtAry = (Point*) new char[ nGesPoints * sizeof(Point) ];

for ( i = 0; i < nGesPoints; i++ )
{
*pWMF >> nX32 >> nY32;
pPtAry[ i ] = Point( nX32, nY32 );
}
```

nGesPoints * sizeof(Point) will result in an integer wrap if nGesPoints is

(0x100000000 / sizeof(Point)).

Code execution is possible via a function pointer overwrite.

3) As above but for EMR_POLYPOLYGON16 record.

Solution:

These issues have now been resolved; OpenOffice and StarOffice users are strongly recommended to install the relevant patch, available from the OpenOffice and SunSolve websites:

<<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/xprod-StarOffice>>
<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/xprod-StarOffice>

[NEWS] OpenOffice and StarOffice Suites WMF and EMF Vulnerabilities

<<http://download.openoffice.org/2.1.0/index.html>>
<http://download.openoffice.org/2.1.0/index.html>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@xxxxxxxxxxxxxx>>
NGSSoftware Insight Security Research.

The original article can be found at:

<<http://www.ngssoftware.com/advisories/high-risk-vulnerabilities-in-the-staroffice-suite/>>
<http://www.ngssoftware.com/advisories/high-risk-vulnerabilities-in-the-staroffice-suite/>

=====

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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

=====

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.