

Office

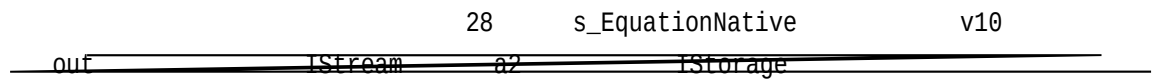
Office (CVE-2017-11882
CVE-2018-0798 CVE-2018-0802) Office
CVE-2018-0798
<http://venustech.com.cn/NewsInfo/4/49366.Html> CVE-2017-
11882 <http://venustech.com.cn/NewsInfo/4/48671.Html>
CVE-2017-11882+CVE-
2018-0802
RTF CVE-2018-
0802

Binary Format) CFBF(Compound File
"\x010le10Native"

URL

CVE-2017-11882 CVE-2018-0802
CFBF Root Entry CLSID {0002CE02-0000-
0000-C000-000000000046}

CLSID Microsoft Equation 3.0 3.0



26~29 CFBF "Equation Native"
 (v11 0) "\x010le10Native"
 35
 "Equation Native" 0x1C
 "\x010le10Native" 4 CVE-2017-11882
 OLE
 38 "\x010le10Native"
 "Equation Native" OLE
 0x001C() 0x00020000()
 40~43
 "\x010le10Native" 4 ([v9+0])

"Equation Native"

0x1C

"\x010le10Native"

4



5

MTEF header (version 2 and later):

The version 2 header consists of a 5-byte header:

byte	description	value
0	MTEF version	3
1	generating platform	0 for Macintosh, 1 for Windows
2	compression method	0 for MTEF, 1 for Equation File
3	product version	3
4	product subversion	0
5	product	

1 3 4

(2) Windows

EQNEDT32.EXE

2

64

32

Office

3

IOC

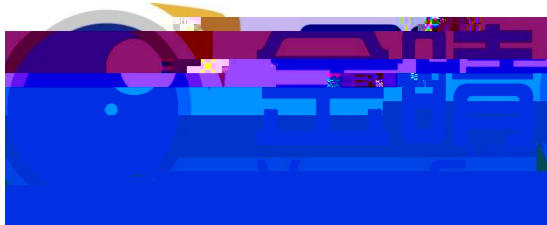
[www\[.\]pensandwoodworking\[.\]com](http://www.pensandwoodworking.com)

[www\[.\]euroasianbridge\[.\]com](http://www.euroasianbridge.com)

[www\[.\]dlpestscontrol\[.\]com](http://www.dlpestscontrol.com)

[www\[.\]salihatasarim\[.\]com](http://www.salihatasarim.com)

www[.]bloggingsays[.]com
www[.]rahafim[.]com



VenusEye
VenusEye

www.venuseye.vip

