Mathcad Security Vulnerability Briefing

Synopsis of Vulnerability

The 'Lock' functionality, used to protect sections Mathcad sheets from alterations, in version 12, 13 and 13.1 is easily bypassed allowing access to the protected data.

The 'Protect Worksheet' functionality is also easily bypassed.

Background on Mathcad

Mathcad (www.mathsoft.com) is used to perform numeric and symbolic calculations, solve differential equations, and handle advanced matrix operations. Mathcad lets you do mathematical calculations on a scratchpad. This turns your screen into a worksheet where you can enter and edit numeric or symbolic calculations, text and graphics anywhere on the document.

Description of Vulnerability

One of the features of Mathcad is allowing the user to define 'Areas'. Mathsoft say that '*You can use areas to protect, lock, or hide information or equations in your worksheets*' and that '*You can also protect the contents within the area, so no one else can edit them*'.

Whilst this is true, it is also very easy to unlock these Areas without needing the password. In the newer versions of Mathcad (12 onwards) the sheets are stored in XML (http://www.w3.org/TR/REC-xml/) format. This provides an easy means of altering the Mathcad sheet, as it is simply plain text. There are 4 vulnerabilities in the way the Area locks work:

1. Password – This attribute is stored as a hashed text string. However the hashes produced for the same word on different sheets are always identical. For example "XfAPUVYgXPg=" represents the string "password", and could be used in any sheet. So it is possible to create another Mathcad sheet, lock an Area with a known password and then use a text editor to copy and paste the known password over the unknown one.
2. Timestamp – Like the password string, this can also be changed to be any value. So the sheet could be unlocked, modified, relocked and then the date of the relocking could be changed to be the original lock date.
3. Complete removal of lock – Inside the Area tag there are is an 'is-locked' attribute. When a lock has been enabled this is set to true. However to remove the lock all that needs to be done is change this value to false. Out of completeness the 'timestamp' attribute should be changed to an empty string and then the 'password' attribute removed. Although these last two changes are not needed to unlock the Area.
4. Protection can be bypassed completely – The data stored in the locked area can also be viewed in a text editor. So this could also be copied and pasted into another sheet, without the lock protection section.

Files may be saved in a 'Compressed XML' format, with a .xmcdz file extension. When opened in a text editor these files are not easily readable. However, if they are opened with an application such as WinRar, then the plain XML file can be extracted and is subject to the vulnerabilities detailed above.

Impact

It is possible for someone to replace the password with one of their own. They can then unlock the area, make changes to the protected data and relock the area. This sheet will then appear to be the same as it was originally, when in fact it could be radically different.

This means that the calculations could be manipulated to produce a desired result when given a certain set of input data.

All of the above vulnerabilities mean that is possible for someone to copy data which was thought safe and read only. This obviously poses a great risk to quality control and also to control of intellectual property rights on Mathcad sheets.

Workaround

None.

Proof of Concept

None required.