Mathcad Security Vulnerability Briefing

Synopsis of Vulnerability

The ‘Protect Worksheet’ functionality, used to protect sections Mathcad sheets from alterations, in versions 12 through 14 is easily bypassed allowing access to the protected data due to the implementation of the file format used to save the files.

Background on Mathcad

Mathcad (http://www.ptc.com/appserver/mkt/products/home.jsp?k=3901) is used to perform, document and share calculation and design work. The unique Mathcad visual format and scratchpad interface integrate standard mathematical notation, text and graphs in a single worksheet - making Mathcad ideal for knowledge capture, calculation reuse, and engineering collaboration.

Vulnerable Software Versions

Mathsoft, Mathcad 12
Mathsoft, Mathcad 13
Mathsoft, Mathcad 13.1
PTC, Mathcad 14

Running on Microsoft, Windows 2000, Service Pack 4
Running on Microsoft, Windows XP, Service Pack 2

Impact

Access Vector:	Locally exploitable.
Access Complexity:	Low.
Authentication:	Not required to exploit.
Impact type:	Provides unauthorised access. Allows partial confidentiality, integrity, and availability violation. Allows unauthorised disclosure of information.

Description of Vulnerability

According to Mathcad’s online help:

‘*When distributing worksheets, you may wish to restrict user access to most regions. Rather than locking an area, you may opt instead to use worksheet protection.*

The intent of file protection is to prevent other users from opening the worksheet in a text editor and editing its contents by hand. The allowed file formats are either binary (XMCDZ, MCD) or output-only (RTF, HTML). With file protection enabled, you can only alter the contents of a worksheet from Mathcad. You can create, edit, and delete regions within the worksheet with no restrictions.’

The XMCDZ file format is not a true binary format. It is the standard Mathcad .XMCD XML sheet, which has been GZIPPED. For this reason it is a simple matter to get the original plain text XML sheet out of the file, using an archive utility.

Once the XML file has been extracted, within the **<editor>** tag there will be a **<protection>** tag. This will look like:
<protection protection-level="low" password="XZEdIlJPXZxa1CQRKn6Sfw=="/>

There are 2 components to this tag; the level of restrictions places upon the sheet and also an optional password needed for un-protecting the sheet.

There are 3 protection-level settings, high, medium and low. These correspond to **Editing**, **Content** and **File** protection, respectively. For example if a sheet was saved with **Editing** protection enabled, then the **<protection>** tag would have a "high" protection level. This can easily be changed with a text editor before the sheet is reopened in Mathcad.

The password is hashed, however the same hash is always produced for a given string. For example "XZEdIlJPXZxa1CQRKn6Sfw==" represents the string "password", and could be used in any sheet.

Due to these limitations the entire **<protection>** tag could be removed, the level of protection could be reduced, or the password could be changed.

The MCD format is a proprietary binary type format. It was used in older version of the application, before the XML format became the standard. However if this format is selected from a newer version of the application, a warning is generated stating that 'If your worksheet is saved as a Mathcad 11 file, some features and calculations may not be preserved'. Selecting either Mathcad 11 or Mathcad 12 MCD file formats produces a warning about potential loss of functionality.

The sheets do include an MD5 hash, however this is only used internally by the application to determine if the sheet has been changed outside of Mathcad and the equations require recalculating. Changing the **<protection>** tag in the XML file will not be detected by the application, and no exceptions will be raised.

Workaround

None.

Proof of Concept

None required.