SCAP, RM & FOUNDSTONE TEST MATRIX GENERATOR

Developer: ***Rioja, Saul***

Manager: ***Guzman, Dorian***

Tools & Automation Team, McAfee Labs Chile

Santiago Chile – October 2011

1. TEST MATRIX APPLICATION

Test Matrix (TM) application was developed by the Tools and Automation Team in McAfee Labs Chile. It allows the SCAP and Foundstone team generate the TM automatically. This task is performed monthly when we receive the bulletins from the VSP program.

1.1 HOW TO EXECUTE

1.1.1. Download the VSP Bulletins (.zip). Extract all bulletins(*.docx) that are in the zip file (You could use the BulletinUncompressor Tool to do it).
1.1.2. Execute TMApplication.exe
1.1.3. Once the application is opened, you have to select the type of Test Matrix you would like to generate (SCAP TM or Foundstone TM).
1.1.4. Select Bulletins location, which is the uncompressed folder in step 1.
1.1.5. Press "Start Generating TM" button.

1.2 TEMPLATES REQUIRED

TM application uses templates to generate the results, so the following templates must in the same folder as the TMApplication.exe:

- ✓ OriginalTM.xlsx: This template is being used to generate the Test Matrix.
- ✓ Apps.xlsx : This file contains the default platforms of the application.

1.3 DATA EXTRACTION FROM BULLETINS

The following items were designed based on the monthly VSP bulletins that we receive. There might some differences or exceptions added from time to time. If that is the case, the person in charge of generating the TM has to change the data in the bulletins manually if necessary.

1.3.1 SCAP

The first thing we do is traverse all the tables that are in each bulletin. The tables that considered have four or five columns and the last three columns of the header's table must have the content highlighted in red.

Operating System		**Maximum Security Impact**	**Aggregate Severity Rating**	**Bulletins Replaced by this Update**
Other Software		**Maximum Security Impact**	**Aggregate Severity Rating**	**Bulletins Replaced by this Update**
Operating System	**Component**	**Maximum Security Impact**	**Aggregate Severity Rating**	**Bulletins Replaced by This Update**
Microsoft Office Suite and Other Software	**Component**	**Maximum Security Impact**	**Aggregate Severity Rating**	**Bulletins Replaced by this Update**

The first column will determine where the content will be placed. It could be the P*latform* or *Component* column. If the fist column contains “Operating System”, the content will be place in the *Platform* column, otherwise it will be placed in the C*omponent* column.

More than one component in the same cell

Whenever we have more than one component in the same cell, the content has to follow the following format:

Format	Example
Abcabcabc (KB#######) Abcabcabc (KB#######)	Microsoft .NET Framework 1.1 Service Pack 1 (KB2572067) Microsoft .NET Framework 2.0 Service Pack 2 (KB2572075) Microsoft .NET Framework 4 (KB2572078)

The cell that contains the KB is the content that we extract

Whenever we are dealing with a table that does not contain “Operating system” in the header, the data that we extract could be either in the first or second column. The element that determines the one we chose is the KB. If the KB is in the first column, that is the column we extract the data from. Otherwise, we extract the data from the second column.

Microsoft Office Suite and Other Software	Component	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Office 2010 and Microsoft Office 2010 Service Pack 1 (32-bit editions)	Microsoft Pinyin IME 2010 (32-bit version) (KB2583956)	Elevation of Privilege	Important	None

Exception

As you can see in the following Table, the relevant content is not where the KB is located (not often, but happens). In order to deal with this exception, you have to have "Microsoft Office SharePoint Server 2007 Service Pack 2 (32-bit editions)" loaded in the Apps.xlsx. Otherwise the content extracted will be “Excel Services”.

Microsoft Office Suite and Other Software	Component	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Office SharePoint Server 2007 Service Pack 2 (32-bit editions)	Excel Services[2] (KB2553093)	Remote Code Execution	Important	MS11-045

1.3.2 FOUNDSTONE

Foundstone's Test Matrix contains the same data as SCAP's TM, so the rules that are explained above apply for Foundstone's TM as well. However, Foundstone TM also extracts data from another table(s); we call it "CVE table". The CVE table has to have one column in the header, and that cell must contain "Vulnerability Severity Rating and Maximum Security Impact by Affected Software".

Vulnerability Severity Rating and Maximum Security Impact by Affected Software		
Affected Software	**.NET Framework Class Inheritance Vulnerability - CVE-2011-1253**	**Aggregate Severity Rating**
Microsoft .NET Framework 1.0 Service Pack 3		
Microsoft .NET Framework 1.0 Service Pack 3 on Windows XP	**Critical** Remote Code Execution	**Critical**

In the CVE table, only cells that contain the following words are the ones taken into account: "Important", "Low", "Critical", and "Moderate". These are the cells that we try to match with the data obtain from previous tables.