Besuchen Sie uns im Internet unter
http://www.vobs.at/rb

Autor: Erich Vonach
6900 Bregenz, Römerstraße 14

RB-Serverpatch ***Security-Follina***

Vorbemerkung

Eine neuer Zero-Day-Bug bei der Remote-Code-Ausführung in Microsoft Office sorgt zurzeit (Anfang Juni 2022) für Wirbel. Genauer gesagt handelt es sich wahrscheinlich um eine Sicherheitslücke bei der Codeausführung, die über Office-Dateien ausgenutzt werden kann. Nach allem, was bislang bekannt ist, gibt es eventuell aber auch andere Möglichkeiten, diese Schwachstelle auszulösen oder zu missbrauchen. Der Sicherheitsforscher Kevin Beaumont hat der Lücke den Namen „Follina" gegeben, der sich als nützlicher Suchbegriff zu dem Thema erweist, bis eine offizielle CVE-Nummer vergeben ist.

- Remote und ohne Makros zum Hackerglück – Zero-Day-Lücke „Follina" in MS Office – Sophos News
- https://news.sophos.com/de-de/2022/05/31/remote-und-ohne-makros-zum-hackerglueck-zero-day-luecke-follina-in-ms-office/

Lösung

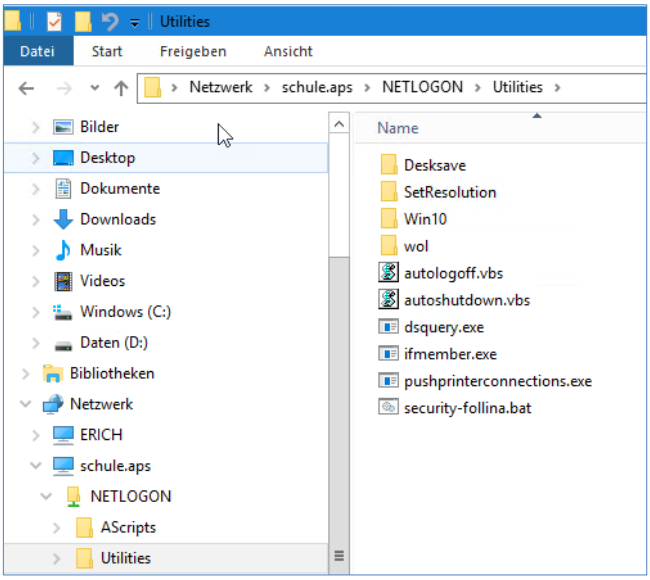
Microsoft empfiehlt das Löschen des Registry-Eintrags HKEY_CLASSES_ROOT\ms-msdt.
Dieser Eintrag verknüpft Dateien dieses Typs mit dem Microsoft Support Diagnostic Tool, was dann der Grund allen Übels ist.

To Do

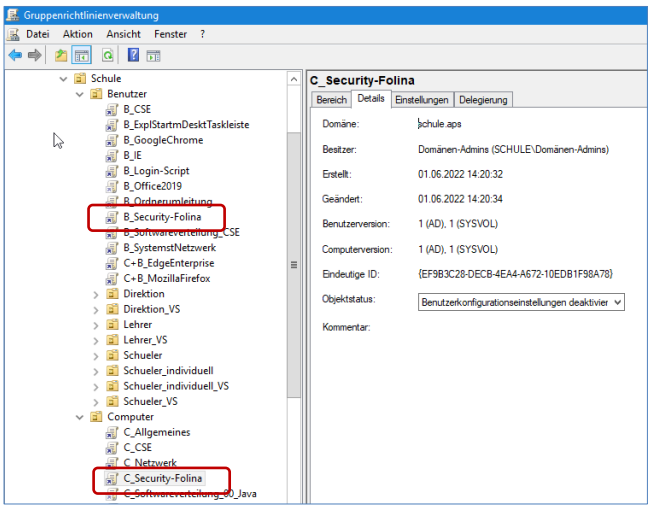
- Kopie des Paketes an einen beliebigen Ort auf dem Server (z.B. *C:\Temp*)
- Ausführen der Datei ***copy_Import.bat***. Folgendes wird automatisch ausgeführt:
  - Kopie der Skriptdate *security-folina.*bat nach *\\schule.aps\netlogon\Utilities*
  - Erstellen von zwei Gruppenrichtlinienobjekten *B_Security-folina* und *B_security-folina* in den ebtsprechenden OUs.

ToDo – Händisch

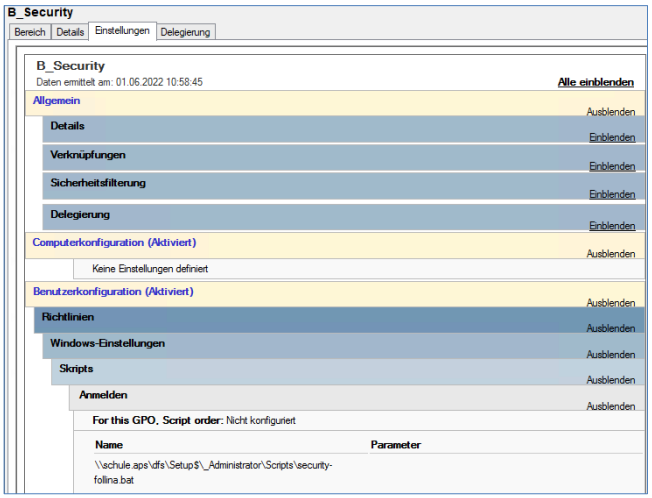
Kopie der Datei *security-folina.bat* nach *\\schule.aps\netlogon\Utilities*



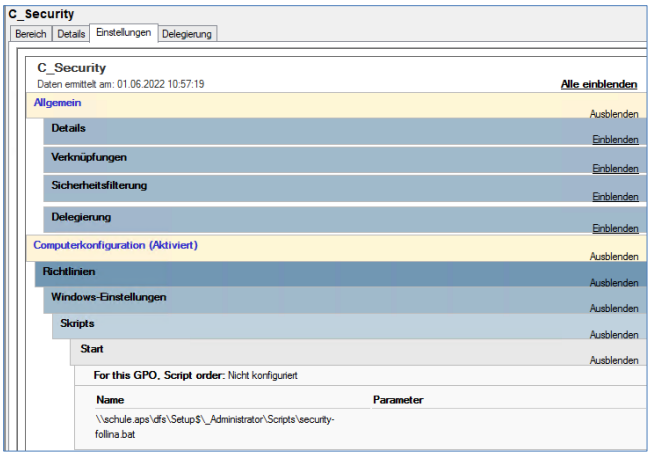
Erstellen zweier Gruppenrichtlinienobjekt *B_Security-folina* und *C_Security-folina* in den entsprechenden OUs.



In B_Security wird das gleiche Skript in Richtlinien → Windows-Einstellungen → Skripts → Anmelden aufgerufen:



In C_Security wird das Skript (security-follina.bat) in Richtlinien → Windows-Einstellungen → Skripts → Start aufgerufen:



Was macht das Skript?

Der erste Skriptaufruf (egal ob im Computer- oder Userkontext) erzeugt das Unterverzeichnis für das Backup des Registryeintrags, wenn es nicht bereits existiert. Ich habe es mal in Logs verfrachtet - ob das schlau ist, mögen bitte auch die Standardinstallationsspezialisten entscheiden.

```
set BACKUPVERZEICHNIS=\\schule.aps\dfs\Logs\security-follina
set BACKUPREGDATEI=%BACKUPVERZEICHNIS%\%COMPUTERNAME%.reg

if NOT EXIST %BACKUPVERZEICHNIS%\ mkdir %BACKUPVERZEICHNIS%
```

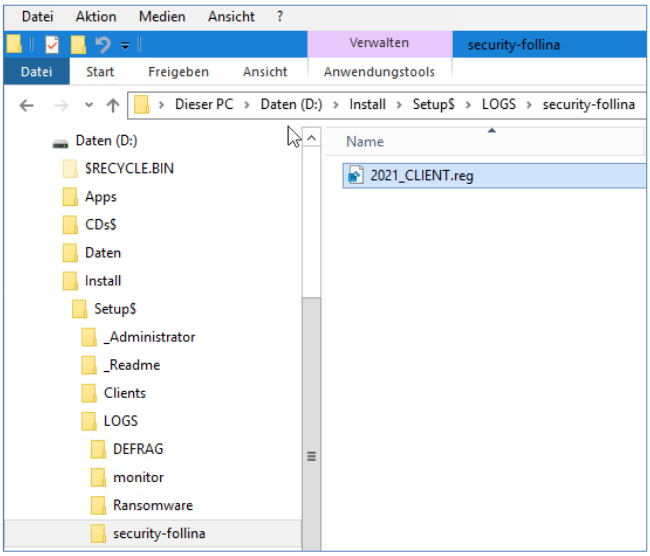
Existiert die Backupdatei noch nicht, dann wird sie erstellt. Der Zugriff auf HKEY_CLASSES_ROOT ist allerdings erst NACH der Benutzernameldung möglich, da dieser Registryzweig aus den Infos der Benutzereinstellungen und der Computereinstellungen zusammengesetzt wird, wobei die Benutzereinstellungen priorisiert werden.
Das heißt, dass dieses Backup erst nach einer Benutzeranmeldung an diesem Computer erstellt wird.

```
if NOT EXIST %BACKUPREGDATEI% reg export HKEY_CLASSES_ROOT\ms-msdt %BACKUPREGDATEI%
```

Wenn das Backup erstellt wurde, werden die unsicheren Registryeinträge gelöscht. Da diese Einträge jedoch in der Standardeinstellung (und die hat in diesem Bereich sicher niemand geändert) aus dem Computerzweig der Registry kommen, hat der User keine Rechte diese zu löschen. Diese werden daher erst beim nächsten Neustart des Computers gelöscht.
Sollte aber möglicherweise tatsächlich ein User den Eintrag geändert haben, wird dieser über den ersten Befehl entfernt. Normalerweise greift aber die zweite Zeile, die es beim Start des Computers (da gibt es HKEY_CLASSES_ROOT ja noch nicht) direkt aus HKLM löscht.

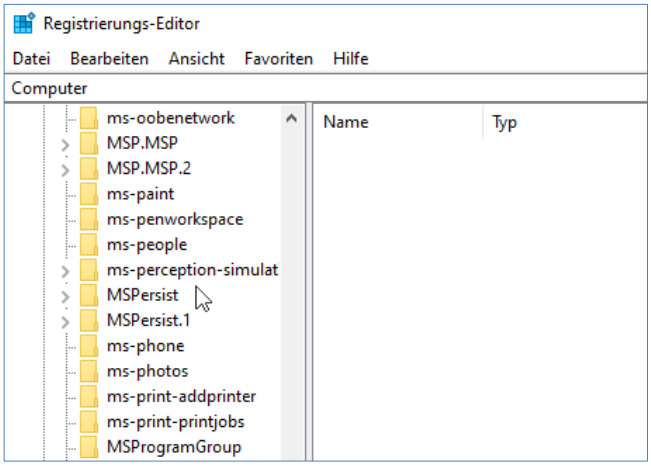
```
if EXIST %BACKUPREGDATEI% reg delete HKEY_CLASSES_ROOT\ms-msdt /f
if EXIST %BACKUPREGDATEI% reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ms-msdt /f
```

Backup des Registry-Schlüssels



Der Sinn des Backups liegt darin, dass auf ähnliche Weise danach die Einstellung wieder eingerichtet werden kann, sobald Microsoft die Lücke geschlossen hat. Daher speichert das Skript auch die Einstellungen mit dem Computernamen ab, auch wenn vermutlich alle Einstellungen gleich sind.

`HKEY_CLASSES_ROOT\ms-msdt`



`HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ms-msdt`