Rechteausweitung mittels Antivirensoftware

Eine Schwachstelle in der Softwarekomponente* McAfee Security Agent*, die unter anderem Bestandteil der Antivirensoftware* McAfee VirusScan Enterprise *ist, kann für Angriffe in Unternehmensnetzwerken genutzt werden.

Dipl.-Inform. Matthias Deeg
Dipl.-Inform. Sebastian Schreiber

26. Januar 2011

1 Einleitung

Endpoint Protection-Software, wie beispielsweise Antivirensoftware, wird heutzutage im Unternehmensumfeld auf nahezu allen Client-Systemen und auf einem Großteil der Server-Systeme mit Windows-Betriebssystem eingesetzt.

Dass diese Softwareprodukte, die für mehr Sicherheit sorgen sollen, selbst nicht frei sind von Schwachstellen, die missbräuchlich durch Angreifer ausgenutzt werden können, wurde in den vergangenen Jahren immer wieder aufs Neue demonstriert (vgl. [1]).

Die SySS GmbH konnte bei einer Analyse der Antivirensoftware McAfee VirusScan Enterprise (VSE) eine Schwachstelle innerhalb der Softwarekomponente McAfee Security Agent (MSA) finden, die seit mehreren Jahren in verschiedenen Softwareversionen dieses Produkts existiert und sich unter gewissen Voraussetzungen zur Rechteausweitung (*Privilege Escalation*) in Unternehmensnetzwerken eignet.

Der McAfee Security Agent ist nach Informationen von McAfee die Client-Komponente des McAfee ePolicy Orchestrator (ePO), welcher für die zentrale Verwaltung verschiedener McAfee-Softwareprodukte eingesetzt werden kann. Die im Folgenden beschriebene Schwachstelle ist somit kein Sicherheitsproblem der Antivirensoftware McAfee VirusScan Enterprise, sondern ein Sicherheitsproblem der genutzten Softwarekomponente McAfee Security Agent, die auch von anderen McAfee-Softwareprodukten genutzt wird.

2 Sicherheitsanalyse

Im Unternehmensumfeld ist es nicht ungewöhnlich, dass Installationen von *Endpoint Protection*-Software ihre Softwareupdates nicht direkt über das Internet, sondern über einen lokalen Updateserver beziehen.

Die Softwarekomponente McAfee Security Agent, die unter anderem Bestandteil der Antivirensoftware McAfee VirusScan Enterprise ist, speichert Konfigurationsinformationen für die *AutoUpdate Repository*-Liste[1] in zwei XML-Dateien namens `SiteList.xml` und `ServerSiteList.xml`. Diese beiden Konfigurationsdateien befinden sich bei der aktuellen Softwareversion McAfee VirusScan Enterprise 8.7.0i im Verzeichnis

```
%AllUsersProfile%Anwendungsdaten\McAfee\Common Framework\
```

und sind für jeden Benutzer lesbar, der Zugriff auf das Windows-System besitzt, wie Abbildung 1 illustriert.

[1] Quellen für die Update-Funktion der Antivirensoftware, z.B. FTP-Server oder Netzlaufwerke

Abbildung 1: Lesender Zugriff auf die Datei `SiteList.xml` für jeden Benutzer

Die Passwortinformationen für verschiedene *Repository* (FTP, HTTP, UNC oder lokale Pfade) sowie für Proxy-Server werden dabei verschlüsselt und in *Base64*-kodierter Form gespeichert.

Im Folgenden wird der Inhalt einer Beispieldatei `SiteList.xml` dargestellt:

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <ns:SiteLists xmlns:ns="naSiteList" GlobalVersion="20030131003110"
3  LocalVersion="20101203081306" Type="Client">
4    <SiteList Default="1" Name="SomeGUID">
5      <HttpSite Type="repository" Name="NAIHttp" Order="1" Enabled="1"
6      Local="1" Server="update.nai.com:80">
7        <RelativePath>products/commonupdater</RelativePath>
8        <UseAuth>0</UseAuth>
9        <UserName></UserName>
10       <Password Encrypted="1">
11         f2mwBTzPQdtnY6QNOsVexH9psAU8z0HbZ2OkDTrFXsR/abAFPM9B3Q==
12       </Password>
13     </HttpSite>
14     <FTPSite Type="repository" Name="NAIFtp" Order="2"
```

```
15      Server="ftp.nai.com:21" Enabled="1" Local="1">
16        <RelativePath>CommonUpdater</RelativePath>
17        <UserName>anonymous</UserName>
18        <Password Encrypted="1">
19          MQCBNesmh4xsoov8E4KA/i9ukpwRoD3RDId9bU+InCJ/abAFPM9B3Q==
20        </Password>
21      </FTPSite><UNCSite Type="repository" Name="Enterprise Repository"
22      Order="3" Server="10.0.23.42" Enabled="1" Local="1">
23        <ShareName>repository$</ShareName>
24        <RelativePath>mcafee</RelativePath>
25        <UseLoggedonUserAccount>0</UseLoggedonUserAccount>
26        <DomainName>Domain</DomainName>
27        <UserName>AV-ADMIN</UserName>
28        <Password Encrypted="1">
29          b2X6AfVMW6RbN+PSiUDCCn9psAU8z0HbZ2OkDTrFXsR/abAFPM9B3Q==
30        </Password>
31      </UNCSite>
32      <ProxyConfigList>
33        <ProxyConfig Name="" UseIEConfig="1" Local="1">
34          <AllowUserToConfigureProxy>0</AllowUserToConfigureProxy>
35          <BypassLocalAddress>0</BypassLocalAddress>
36          <ExclusionList/><FtpUseAuth>0</FtpUseAuth>
37          <HttpUseAuth>0</HttpUseAuth>
38          <HttpProxyUser></HttpProxyUser>
39          <HttpProxyPassword Encrypted="1">
40            f2mwBTzPQdtnY6QNOsVexH9psAU8z0HbZ2OkDTrFXsR/abAFPM9B3Q==
41          </HttpProxyPassword>
42          <FtpProxyUser></FtpProxyUser>
43          <FtpProxyPassword Encrypted="1">
44            f2mwBTzPQdtnY6QNOsVexH9psAU8z0HbZ2OkDTrFXsR/abAFPM9B3Q==
45          </FtpProxyPassword>
46          <AlternateFtpUseAuth>0</AlternateFtpUseAuth>
47          <AlternateHttpUseAuth>0</AlternateHttpUseAuth>
48          <AlternateHttpProxyUser></AlternateHttpProxyUser>
49          <AlternateHttpProxyPassword Encrypted="1">
50            f2mwBTzPQdtnY6QNOsVexH9psAU8z0HbZ2OkDTrFXsR/abAFPM9B3Q==
51          </AlternateHttpProxyPassword>
52          <AlternateFtpProxyUser></AlternateFtpProxyUser>
53          <AlternateFtpProxyPassword Encrypted="1">
54            f2mwBTzPQdtnY6QNOsVexH9psAU8z0HbZ2OkDTrFXsR/abAFPM9B3Q==
55          </AlternateFtpProxyPassword>
56        </ProxyConfig>
57      </ProxyConfigList>
58    </SiteList>
59  </ns:SiteLists>
```

Listing 1: Inhalt der Konfigurationsdatei `SiteList.xml`

Eine Analyse der verwendeten Verschlüsselungsmethode für die Passwortinformationen durch die SySS GmbH ergab, dass der Verschlüsselungsalgorithmus *Triple DES* (3DES)[2] in Kombination mit einer einfachen XOR-Verschlüsselung eingesetzt wird. Besonders

[2] nähere Informationen unter `http://de.wikipedia.org/wiki/Data_Encryption_Standard`

interessant ist dabei die Feststellung, dass sowohl das Schlüsselmaterial für die 3DES- als auch für die XOR-Verschlüsselung statisch ist.

Weitere Untersuchungen durch die SySS GmbH ergaben, dass die Passwortinformationen der Konfigurationsdateien bei den folgenden Softwareversionen alle mit demselben Schlüsselmaterial verschlüsselt werden:

- McAfee VirusScan Enterprise 7.1.0
- McAfee VirusScan Enterprise 8.0.0i
- McAfee VirusScan Enterprise 8.5.0i
- McAfee VirusScan Enterprise 8.7.0i

Die Tatsache, dass jeder Benutzer lesenden Zugriff auf die Konfigurationsdateien von McAfee VirusScan Enterprise beziehungsweise der genutzten Softwarekomponente McAfee Security Agent besitzt, in denen sich im Unternehmensumfeld mit hoher Wahrscheinlichkeit Anmeldedaten für interne Update- oder Proxy-Server befinden, kombiniert mit der Verwendung statischen Schlüsselmaterials, ermöglicht unter gewissen Voraussetzungen die Durchführung von *Privilege Escalation*-Angriffen.

Bei dieser Form des Angriffs ist das Ziel eines Angreifers seine Berechtigungen auszuweiten. Im Kontext von Windows-Domänen innerhalb von Unternehmensnetzwerken kann dies beispielsweise durch das Ermitteln von Anmeldedaten fremder Domänen-Benutzerkonten geschehen. Für einen Angreifer besonders interessant sind dabei Benutzerkonten für *Software Deployment-* und *Endpoint Protection*-Lösungen, wie beispielsweise die Antivirensoftware McAfee VirusScan Enterprise, da diese Benutzerkonten oftmals über höhere Berechtigungen verfügen, um administrative Aufgaben erfüllen zu können.

Die verschlüsselten Passwortinformationen in den Konfigurationsdateien, die möglicherweise für *Privilege Escalation*-Angriffe nützlich sind, können auf sehr einfache Weise entschlüsselt und im Klartext eingesehen werden. Ein Angreifer muss dazu lediglich die entsprechenden Konfigurationsdateien kopieren, in eine eigene Installation von McAfee VirusScan Enterprise importieren[3] und anschließend die verdeckt angezeigten Passwörter mit einem *Password Revealer*[4] aufdecken.

Abbildung 2 zeigt die Einstellungen eines Beispiel-*Repository* mit dem Namen `Enterprise Repository` einmal mit verdeckten und einmal mit aufgedeckten Passwortinformationen für den Benutzer `AV-ADMIN`.

[3] Evaluationsversionen können kostenlos von McAfee bezogen werden
[4] z.B. `http://win32assembly.online.fr/files/revealer.zip`

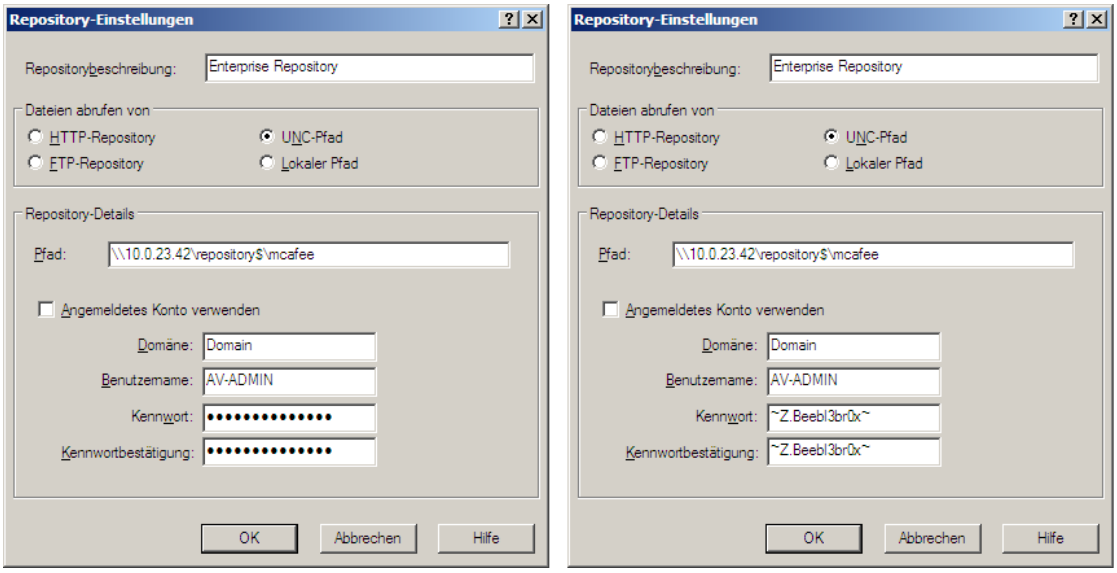

Abbildung 2: Einstellungen des *Repository* `Enterprise Repository` mit verdeckten und via *Password Revealer* aufgedeckten Passwortinformationen

Des Weiteren entwickelte die SySS GmbH ein Softwaretool namens McAfee Password Decryptor, das unabhängig von einer McAfee VirusScan Enterprise-Installation in der Lage ist, sämtliche Passwortinformationen der Konfigurationsdateien `SiteList.xml` und `ServerSiteList.xml` im Klartext wiederherzustellen.

Die folgende Ausgabe dieses Softwaretools zeigt beispielhaft die Entschlüsselung von Passwortinformationen einer Konfigurationsdatei von McAfee VirusScan Enterprise 8.7.0i.

```
$ ./mpd.py SiteList.xml
                _____________________________________________________________
               /    _____       _____ _____                                  \
              /    /  ___|     /  ___/  ___|                                  \
             |     \ `--. _   _\ `--.\ `--.                                    |
             |      `--. \ | | |`--. \`--. \                                   |
             |     /\__/ / |_| /\__/ /\__/ /                                   |
              \    \____/ \__, \____/\____/   ... decrypts your passwords!    /
               \           __/ |                                             /
                /         |___/    _____________________________________/
               / ________________/
        (__) /_/
        (oo)
  /------\/
 / |____||
*  ||   ||
   ^^   ^^
McAfee Password Decryptor v1.0 by Matthias Deeg <matthias.deeg@syss.de> - SySS GmbH (c) 2010
[*] Found 3 user credentials in SiteList.xml

Username                Password                                Account Type
-------------------------------------------------------------------------------------------------------
anonymous               CommonUpdater@McAfeeB2B.com             FTP (NAIFtp, ftp.nai.com:21)
<empty>                 <empty>                                 HTTP (NAIHttp, update.nai.com:80)
AV-ADMIN                ~Z.Beebl3br0x~                          UNC (Enterprise Repository,
                                                                \\10.0.23.42\repository$\mcafee)
```

Im Rahmen durchgeführter Penetrationstests war es der SySS GmbH möglich, unter Ausnutzung der beschriebenen Schwachstelle erfolgreich *Privilege Escalation*-Angriffe in Unternehmensnetzwerken durchzuführen, die bis hin zu den Berechtigungen eines *Enterprise*-Administrators für Windows-Domänen reichten.

3 Fazit

Nach Auffassung der SySS GmbH stellt die gefundene Schwachstelle ein hohes Sicherheitsrisiko dar, da mit deren Ausnutzung unter gewissen Voraussetzungen *Privilege Escalation*-Angriffe in Unternehmensnetzwerken möglich sind, die bis hin zu administrativen Berechtigungen für die gesamte Windows-Domäne reichen können.

Der Zugriff auf Passwortinformationen, auch wenn diese verschlüsselt sind, sollte generell soweit wie möglich eingeschränkt werden. Konfigurationsdateien, die von allen Benutzern eines Systems gelesen werden können, sind ein denkbar ungeeigneter Speicherort für solche Daten.

Darüber hinaus erleichtert die Tatsache, dass für verschiedene Softwareversionen von McAfee VirusScan Enterprise beziehungsweise für verschiedene Softwareversionen der verwendeten Softwarekomponente McAfee Security Agent seit mehreren Jahren

dieselbe Verschlüsselungsmethode mit demselben Schlüsselmaterial verwendet wird, die Durchführung von *Privilege Escalation*-Angriffen sehr.

Der SySS GmbH sind neben der Antivirensoftware McAfee VirusScan Enterprise noch weitere Softwareprodukte anderer Hersteller bekannt, die von einer Variante der beschriebenen Schwachstelle betroffen sind. Der Zugriff auf Passwortinformationen, sowohl auf Client- als auch auf Server-Systemen, wie beispielsweise Microsoft Terminal Server-Systemen, lässt sich dabei unter gewissen Voraussetzungen ebenfalls durch eingeschränkte Benutzer für *Privilege Escalation*-Angriffe in Unternehmensnetzwerken nutzen.

Die SySS GmbH empfiehlt, für den Zugriff auf Software-Updates keine administrativen Benutzer, sondern lediglich Benutzer mit sehr eingeschränkten Rechten zu verwenden (*Least-Privileged User Account [LUA]*), um generell die Möglichkeiten von *Privilege Escalation*-Angriffen bei Zugriff auf entsprechende Passwortinformationen einzuschränken.

Der Softwarehersteller McAfee wurde von der SySS GmbH über das gefundene Sicherheitsproblem in Kenntnis gesetzt. McAfee hat schnell reagiert und einen *Knowledge Base*-Artikel mit dem Titel *Important information on using Download Credentials* veröffentlicht (siehe [2]), in dem die sichere Konfiguration der betroffenen Softwarekomponente McAfee Security Agent beschrieben wird. Des Weiteren werden nach Informationen von McAfee mögliche zukünftige Software-Updates, die die beschriebene Sicherheitsschwäche betreffen, ebenfalls in diesem *Knowledge Base*-Artikel aufgeführt.

Literatur

[1] Jürgen Schmidt, *Antivirus software as a malware gateway*, `http://www.h-online.com/security/features/Antivirus-software-as-a-malware-gateway-746143.html` 2

[2] *Knowledge Base*-Artikel von McAfee, *Important information on using Download Credentials*, `https://kc.mcafee.com/corporate/index?page=content&id=KB70999` 8