Privilege Escalation via Antivirus Software

A security vulnerability in the software component* McAfee Security Agent*, which is part of the antivirus software* McAfee VirusScan Enterprise*, can be leveraged in attacks against corporate networks.

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

January 26, 2011

1 Introduction

Today almost every client system and the majority of server systems in enterprise environments are protected by endpoint protection software, e.g. antivirus software, especially when Windows operating systems are in use.

In recent years, it has been shown more than once that these protective software products sometimes also have severe security vulnerabilities which can be exploited by attackers (cf. [1]).

In a security analysis of the antivirus software McAfee VirusScan Enterprise (VSE), the SySS GmbH could find a security vulnerability in the software component McAfee Security Agent (MSA) which can be used under certain conditions in order to perform *privilege escalation attacks* within corporate networks. Several software versions of McAfee VirusScan Enterprise are affected by this security issue.

According to McAfee, the McAfee Security Agent is the client component of the McAfee ePolicy Orchestrator (ePO), a central console which can be used to manage several McAfee software products. Therefore, the security vulnerability described below is not a security issue of the antivirus software McAfee VirusScan Enterprise, but a security issue of the used software component McAfee Security Agent which is part of McAfee VirusScan Enterprise but also used by other McAfee software products.

2 Security Assessment

In enterprise environments, it is not unusual that software updates for endpoint protection software are not downloaded via the Internet from external sources by each software installation but that software updates are provided by a local update server within the corporate network.

The software component McAfee Security Agent which is used for managing software updates of the antivirus software McAfee VirusScan Enterprise stores the configuration settings of the *AutoUpdate repository list*[1] in two XML files named `SiteList.xml` and `ServerSiteList.xml`. In the current software version McAfee VirusScan Enterprise 8.7.0i, these two configuration files are located in the directory

```
%AllUsersProfile%Application Data\McAfee\Common Framework\
```

and they can be read by every user who has access to the Windows system, as figure 1 illustrates.

[1] repositories for the update function, e.g. FTP servers or network shares

Figure 1: Read access for the file `SiteList.xml` for every user (German WINDOWS)

The password information for different repositories (FTP, HTTP, UNC or local paths) as well as for proxy servers are encrypted and stored as *base64*-encoded value.

The following listing shows the content of a sample configuration file `SiteList.xml`:

```
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: Content of a sample configuration file `SiteList.xml`

An analysis of the used encryption method by the SySS GmbH showed, that the encryption algorithm *Triple DES* (3DES)[2] in combination with a simple XOR encryption is used. The fact that not only the encryption key for the 3DES but also for the XOR encryption is static, is of particular interest.

[2]further information can be found at `http://de.wikipedia.org/wiki/Data_Encryption_Standard`

Further investigations by the SySS GmbH showed that the password information of the following software versions are all encrypted with the same encryption keys:

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

The fact that every user can read the configuration files of the McAfee VirusScan Enterprise installation respectively the McAfee Security Agent, in which user credentials for internal update or proxy servers are stored with a very high probability in enterprise environments, makes it possible to perform *privilege escalation attacks* under certain conditions.

In this kind of attack, the attacker elevates his privileges in order to gain access to resources he usually has no access to. In the context of a Windows domain within a corporate network, for example, an attacker can elevate his privileges by stealing credentials of other domain users. Especially user accounts for software deployment and endpoint protection software are interesting targets for such an attack, as these user accounts usually have higher privileges in order to accomplish administrative tasks.

The encrypted password information in the configuration files, which are possibly useful for *privilege escalation attacks*, can be decrypted very easily. An attacker only has to copy the corresponding configuration files, import them in an installation of McAfee VirusScan Enterprise[3] of his own and afterwards reveal the passwords with a *password revealer*[4] of his choice.

Figure 2 shows the configuration of a sample repository named `Enterprise Repository` with and without revealed password information for the user `AV-ADMIN`.

[3] Evaluation versions can be obtained from McAfee free of charge
[4] e.g. `http://win32assembly.online.fr/files/revealer.zip`

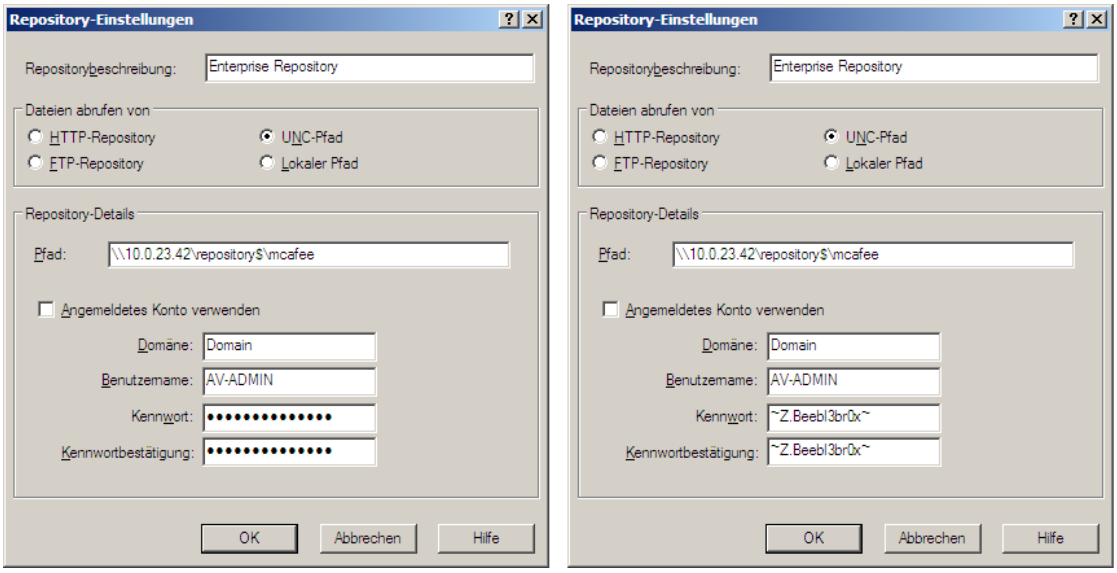

Figure 2: Configuration of the sample repository `Enterprise Repository` with and without revealed password information

Furthermore, the SySS GmbH developed a software tool called McAfee Password Decryptor which is able to decrypt all password information of the configuration files `SiteList.xml` and `ServerSiteList.xml` independent of a McAfee VirusScan Enterprise installation.

The following output of this software tool shows the decryption of password information of a configuration file copied from a McAfee VirusScan Enterprise 8.7.0i installation.

```
$ ./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)
```

In the course of conducted security assessments, the SySS GmbH could successfully perform *privilege escalation attacks* within corporate networks by exploiting the described security vulnerbality in order to gain administrative privileges for Windows domains.

3 Conclusion

The SySS GmbH rates the found security vulnerability as high security risk, because under certain conditions it is possible to perform *privilege escalation attacks* by exploiting this security weakness, which can even result in administrative privileges for Windows domains.

Generally, the access to password information, no matter whether encrypted or not, should be restricted as much as possible. Configuration files that are readable by every system user are not the proper place to store such data.

The fact that different software versions of McAfee VirusScan Enterprise respectively different software versions of the McAfee Security Agent use the same encryption method and the same encryption keys for several years now, facilitates *privilege escalation attacks* concerning this software.

Besides the antivirus software McAfee VirusScan Enterprise, the SySS GmbH knows about further software products of other manufacturers which are also prone to the described type of security vulnerability. Therefore, these software products can also be levereged under certain conditions to gain elevated privileges within corporate networks.

The SySS GmbH recommends to use least-privileged user accounts (LUA) for software updates in order to reduce the risk of possible *privilege escalation attacks* with the access to corresponding password information.

The SySS GmbH contacted the software manufacturer McAfee and informed him about the found security issue. McAfee responded quickly and released a knowledge base article titled *Important information on using Download Credentials* (see [2]) in which the proper and secure configuration of the affected software component McAfee Security Agent is described. Furthermore, according to McAfee any additional code changes concerning this security issue will also be included in an update to this knowledge base article in the future.

References

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