Matthias Deeg

Privilege Escalation via Client Management Software

Security vulnerabilities in the Client Management Software FrontRange DSM can be leveraged in attacks against corporate networks.

Client management is a very important task in modern enterprise IT environments as all computer systems, whether client or server, should be managed throughout their entire system life cycle.

There are many client management software solutions from different vendors that support IT managers and IT administrators in client management tasks like:

- inventory
- patch management
- software deployment
- license management

As a matter of principle, in order to perform these functions, client management software requires high privileges, usually administrative rights, on the managed client and server systems. Therefore, client management software is an interesting target for attackers as vulnerabilities in this kind of software may be leveraged for privilege escalation attacks within corporate networks.

During a penetration test of client and server systems of a corporate network, the SySS GmbH could find multiple security vulnerabilities in the client management software FrontRange Desktop & Server Management (DSM) v7.2.1.2020 [1] that could be successfully exploited in a privilege escalation attack resulting in administrative privileges for the entire Windows domain.

Security Assessment

During a security assessment of a client system managed with FrontRange DSM, the SySS GmbH found out that the client management solution FrontRange DSM stores and uses sensitive user credentials for required user accounts in an insecure manner which enables an attacker or malware with file system access to a managed client, for example with the privileges of a limited Windows domain user account, to recover the cleartext passwords.

The recovered passwords can be used for privilege escalation attacks and for gaining unauthorized access to other client and/or server systems within the corporate network as at least one FrontRange DSM user account needs local administrative privileges on managed systems.

FrontRange DSM stores passwords for different user accounts encrypted in two configuration files named `NiCfgLcl.ncp` and `NiCfgSrv.ncp`.

These configuration files contain encrypted password information for different required FrontRange DSM user accounts (see [2]), for example:

- DSM Runtime Service
- DSM Distribution Service

- Business Logic Server (BLS) Authentication
- Database account

The actual number of required FrontRange DSM user accounts depends on the chosen security level during the software installation as Figure 1 illustrates.

A limited Windows domain user has read access to these configuration files that are usually stored in the following locations:

- `%PROGRAMFILES(X86)\NetInst\NiCfgLcl.ncp` (local on a managed client)
- `%PROGRAMFILES(X86)\NetInst\NiCfgSrv.ncp` (local on a managed client)
- `\\<FRONTRANGE SERVER>\DSM$\NiCfgLcl.ncp` (remote on a DSM network share)
- `\\<FRONTRANGE SERVER>\DSM$\NiCfgSrv.ncp` (remote on a DSM network share)

An analysis of the used encryption method by the SySS GmbH showed, that the passwords are encoded and encrypted using a hard-coded secret (cryptographic key) contained within the FrontRange DSM executable file `NiInst32.exe`.

Furthermore, the SySS GmbH found out that the process `NiInst32.exe`, that is executed in the context of a low-privileged user, decrypts and uses some of the user credentials contained in the FrontRange DSM configuration files. Thus, an attacker or malware running in the same low-privileged user context can analyze and control the process `NiInst32.exe` and in this way gain access to decrypted cleartext passwords.

For instance, such an online attack targeting the running process `NiInst32.exe` can be performed using an application-level debugger like OllyDbg [3] from the perspective of a limited Windows user.

Figure 2 exemplarily shows the successful extraction of the decrypted cleartext password of the FrontRange DSM user account `DSM Distribution Service`. In order to gain ac-

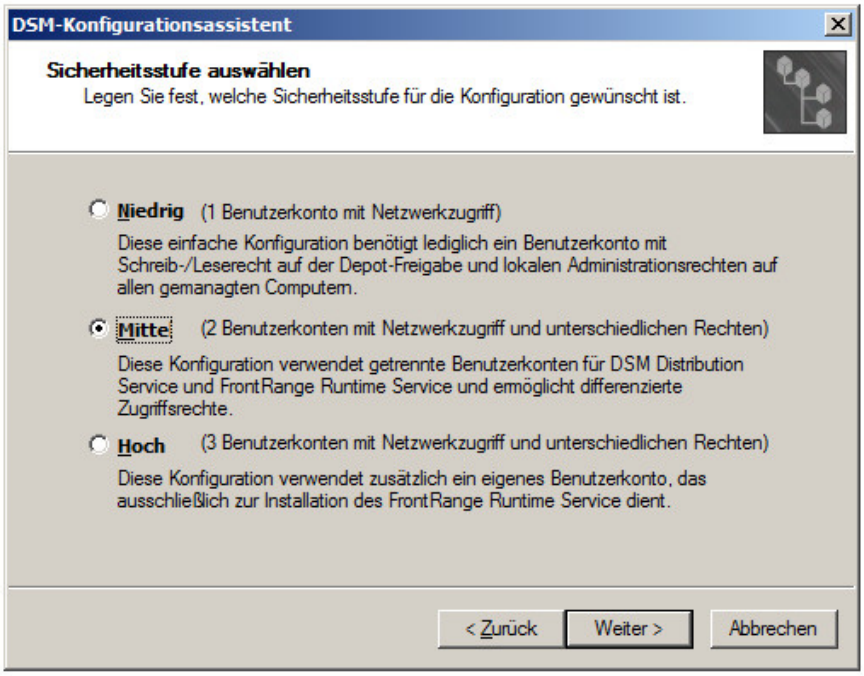

Figure 1: Chosing the security level during the FrontRange DSM software installation which influences the number of required user accounts (one, two, or three)

cess to the decrypted password, it is sufficient to set a breakpoint on the Windows API function `LogonUserW` of the module `ADVAPI32.DLL`.

Another way for an attacker or malware having file system access to the FrontRange DSM configuration files in order to find out the cleartext passwords of the stored user credentials is an offline attack. For this attack, it is required to know how the passwords are actually encoded and encrypted. Fortunately, by having file system access to the target system, an attacker can analyze the client-side components of the client management software FrontRange DSM, like the executable file `NiInst32.exe` or other relevant dynamic link libraries (DLLs) like `icdbclnt.dll`, and find out how the encoding and the encryption is done. With this gained knowledge all stored FrontRangeDSM passwords can be recovered as cleartext.

The SySS GmbH developed a proof-of-concept software tool named `FrontRange DSM Password Decryptor` which is able to decrypt all password information stored within the FrontRange configuration files `NiCfgLcl.ncp` and `NiCfgSrv.ncp`. The following output of this software tool (see Listing 1) shows a successful password recovery.

The described security vulnerabilities could be successfully exploited with the following FrontRange DSM software versions:

- FrontRange DSM v7.2.1.2020
- FrontRange DSM v7.2.2.2331

Listing 1: Successful password recovery using the PoC software tool

```
>fpd.exe k22D01816EADA56F850G09218CCD5GC1C4537FC70768629C14FF5B
FrontRange DSM Password Decryptor v1.0 by Matthias Deeg <matthias.
deeg@syss.de> - SySS GmbH (c) 2014
[+] Decrypted password: I wanna be a pirate!
```

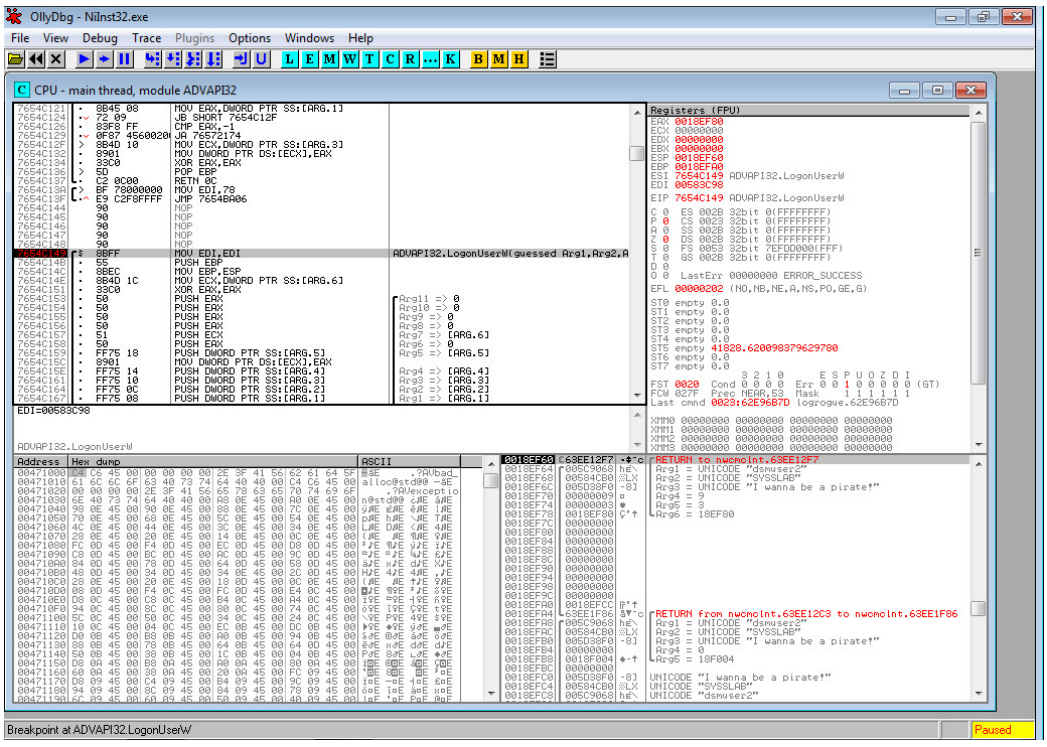

Figure 2: Extracting the decrypted cleartext password of the DSM user account DSM Distribution Service from the memory of the process NiInst32.exe using OllyDbg

Conclusion

The software solution FrontRange DSM insufficiently protects sensitive user credentials and violates secure design principles. Limited user accounts have read access to the stored password information, the passwords can be recovered as cleartext using a hard-coded cryptographic key, and due to the software design, the passwords are also used in the context of a low-privileged user process (`NiInst32.exe`) which can be analyzed and controlled by an attacker or malware running in the same low-privileged user context.

The SySS GmbH rates the found security vulnerabilities as high security risks, because they can be leveraged in a privilege escalation attack which can even result in administrative privileges for entire 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 low-privileged users are not the proper place to store such data, and low-privileged user processes are not the proper place to use them.

A similar security vulnerability affecting the software component McAfee Security Agent, which is part of the antivirus software McAfee VirusScan Enterprise, has been described in our paper *Privilege Escalation via Antivirus Software* [4] from 2011. Another popular security vulnerability similar to the security vulnerabilities described in this paper affects setting passwords via Group Policy Preferences (GPP) of Microsoft Windows Server operating systems that can also leverage privilege escalation attacks [5].

The SySS GmbH recommends to change the software design of the client management software FrontRange DSM, so that sensitive password information is only accessible to and processed by specific, high-privileged user accounts like Windows service accounts running with SYSTEM privileges. In this way, a low-privileged attacker or malware cannot access and recover sensitive password information.

The SySS GmbH contacted the manufacturer FrontRange USA Inc. and informed him about the found security issues via the SySS security advisory SYSS-2014-007 [6]. According to information by FrontRange, the described security vulnerabilities have been fixed in a new software release available on April 30, 2015. Please contact the vendor for further information or support.

References

[1] FrontRange DSM Web site, http://www.frontrange.com/heat/products/client-management

[2] FrontRange DSM Getting Started Guide

[3] OllyDbg Web site, http://www.ollydbg.de/

[4] Matthias Deeg and Sebastian Schreiber, *Privilege Escalation via Antivirus Software,* https://www.syss.de/fileadmin/dokumente/Publikationen/2011/SySS_2011_Deeg_Privilege_Escalation_via_Antivirus_Software.pdf

[5] Microsoft Security Bulletin MS14-025, *Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege (2962486),* https://technet.microsoft.com/en-us/library/security/ms14-025.aspx

[6] *SySS Security Advisory SYSS-2014-007,* https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2014-007.txt