Matthias Deeg

Rechteausweitung mittels Client-Management-Software

Schwachstellen in der Client-Management-Software FrontRange DSM können für Angriffe im Unternehmensnetzwerk genutzt werden.

Client-Management ist eine sehr wichtige Aufgabe in modernen IT-Umgebungen, da alle Computersysteme, egal ob Client- oder Serversysteme, ihren ganzen Lebenszyklus lang verwaltet werden sollten.

Es gibt zahlreiche Client-Management-Software-Lösungen von verschiedenen Herstellern, die IT-Manager und IT-Administratoren bei der Erfüllung von Client-Management-Aufgaben unterstützen, wie zum Beispiel:

- Inventarisierung
- Patch-Management
- Softwareverteilung
- Lizenz-Management

Um diese Funktionen ausführen zu können, benötigt Client-Management-Software prinzipbedingt hohe Privilegien auf den verwalteten Client- und Serversystemen, normalerweise in Form von administrativen Berechtigungen. Deshalb stellt Client-Management-Software ein interessantes Ziel für Angreifer dar, da Schwachstellen in dieser Art von Software möglicherweise für Angriffe zur Rechteausweitung innerhalb von Unternehmensnetzwerken genutzt werden können.

Während eines Sicherheitstests von Client- und Server-Systemen eines Unternehmensnetzwerks fand die SySS GmbH mehrere Schwachstellen in der Client-Management-Software FrontRange Desktop & Server Management (DSM) v7.2.1.2020 [1], die erfolgreich für eine Rechteausweitung ausgenutzt werden konnten und die schließlich in administrativen Berechtigungen für die gesamte Windows-Domäne resultierte.

Sicherheitsanalyse

Im Rahmen des Sicherheitstests eines Client-Systems, das mit FrontRange DSM verwaltet wurde, stellte die SySS GmbH fest, dass die Client-Management-Lösung FrontRange DSM sensible Anmeldedaten für benötigte Benutzerkonten auf unsichere Weise speichert und verwendet. Dadurch wird ein Angreifer oder eine Schadsoftware mit Dateisystemzugriff auf ein verwaltetes Client-System, beispielsweise mit den Berechtigungen eines eingeschränkten Windows-Benutzers, in die Lage versetzt, die Klartextpasswörter wiederherzustellen.

Die in Erfahrung gebrachten Passwörter können für Angriffe zur Rechteausweitung und für den unautorisierten Zugriff auf andere Client- und/oder Serversysteme innerhalb des Unternehmensnetzwerks genutzt werden, da mindestens ein Benutzerkonto von FrontRange DSM lokale administrative Berechtigungen auf den verwalteten Computersystemen benötigt.

FrontRange DSM speichert Passwörter für unterschiedliche Benutzerkonten in verschlüsselter Form in zwei Konfigurationsdateien namens `NiCfgLcl.ncp` und `NiCfgSrv.ncp`. Diese

Konfigurationsdateien enthalten verschlüsselte Passwortinformationen für verschiedene von FrontRange DSM benötigte Benutzerkonten (siehe [2]), wie zum Beispiel:

- DSM Runtime Service
- DSM Distribution Service
- Business Logic Server (BLS) Authentication
- Benutzerkonto für Datenbankzugriff

Die tatsächliche Anzahl an benötigten Benutzerkonten für FrontRange DSM hängt von der gewählten Sicherheitsstufe ab, die während der Softwareinstallation festgelegt wird, wie Abbildung 1 illustriert.

Ein Windows-Domänenbenutzer mit eingeschränkten Berechtigungen hat lesenden Zugriff auf diese Konfigurationsdateien, die für gewöhnlich an folgenden Orten gespeichert sind:

- `%PROGRAMFILES(X86)\NetInst\NiCfgLcl.ncp` (lokal auf einem verwalteten Client-System)
- `%PROGRAMFILES(X86)\NetInst\NiCfgSrv.ncp` (lokal auf einem verwalteten Client-System)
- `\\<FRONTRANGE SERVER>\DSM$\NiCfgLcl.ncp` (entfernt auf einem DSM-Netzlaufwerk)
- `\\<FRONTRANGE SERVER>\DSM$\NiCfgSrv.ncp` (entfernt auf einem DSM-Netzlaufwerk)

Eine Analyse der verwendeten Verschlüsselungsmethode durch die SySS GmbH ergab, dass die Passwortinformationen mit einem statischen Geheimnis (kryptografisches Schlüsselmaterial), das sich in der ausführbaren Datei `NiInst32.exe` von FrontRange DSM befindet, kodiert und verschlüsselt werden.

Des Weiteren stellte die SySS GmbH fest, dass der Prozess `NiInst32.exe`, der im Kontext eines niedrigprivilegierten Benutzers ausgeführt wird, manche der Anmeldedaten, die in den Konfigurationsdateien von FrontRange DSM gespeichert sind, entschlüsselt und verwendet. Dies ermöglicht einem Angreifer oder einer Schadsoftware im selben niedrigprivilegierten Benutzerkontext, den Prozess `NiInst32.exe` zu analysieren und zu kontrollieren, um auf diese Weise Zugriff auf entschlüsselte Klartextpasswörter zu erlangen.

Ein solcher Online-Angriff, der den laufenden Prozess `NiInst32.exe` zum Ziel hat, kann beispielsweise mit Hilfe eines Softwaredebuggers wie OllyDbg [3] aus der Perspektive eines ein-

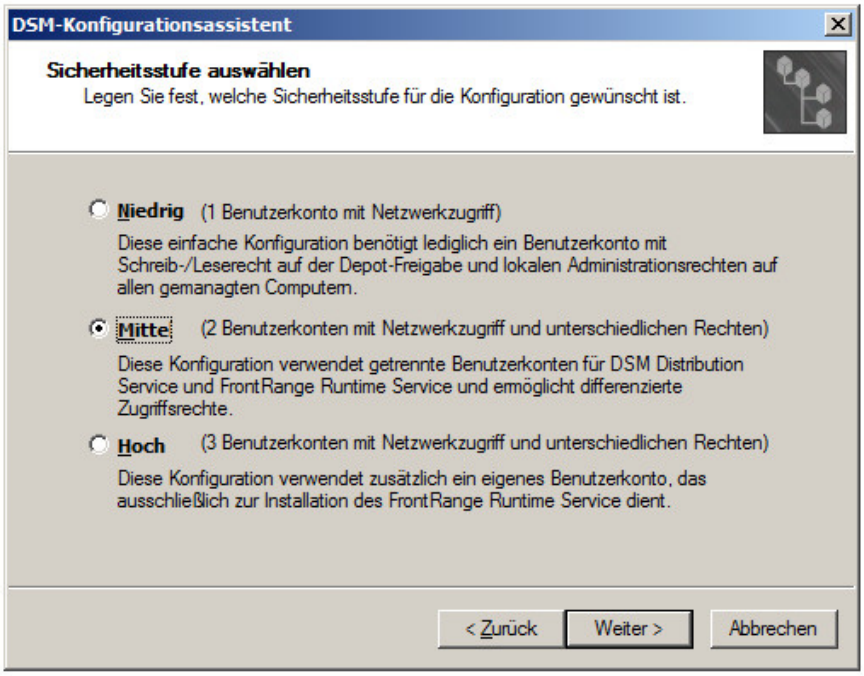

Abbildung 1: Auswahl der Sicherheitsstufe während der Softwareinstallation von FrontRange DSM, die die Anzahl benötigter Benutzerkonten beeinflusst

geschränkten Windows-Benutzers durchgeführt werden.

Abbildung 2 zeigt beispielhaft das erfolgreiche Auslesen des entschlüsselten Klartextpasswortes des FrontRange DSM-Benutzerkontos DSM Distribution Service. Um Zugriff auf das entschlüsselte Passwort zu erhalten, reicht es aus, einen Haltepunkt auf die Windows API-Funktion LogonUserW des Moduls `ADVAPI32.DLL` zu setzen.

Ein anderer Weg für einen Angreifer oder eine Schadsoftware mit Dateisystemzugriff auf die Konfigurationsdateien von FrontRange DSM die Klartextpasswörter der gespeicherten Anmeldedaten in Erfahrung zu bringen, ist eine Offline-Attacke. Für diese Art von Angriff ist es notwendig zu wissen, wie die Passwörter tatsächlich kodiert und verschlüsselt werden. Ein Angreifer mit Dateisystemzugriff auf das Zielsystem kann (un) glücklicherweise die clientseitigen Komponenten der Client-Management-Software FrontRange DSM analysieren, wie etwa die ausführbare Datei `NiInst32.exe` oder andere relevante Programmbibliotheken (DLLs), wie beispielsweise `icdbclnt.dll`, und so die Funktionsweise der Kodierung und der Verschlüsselung herausfinden. Mit diesem Wissen können alle gespeicherten Passwörter von FrontRange DSM im Klartext wiederhergestellt werden.

Die SySS GmbH entwickelte ein Proof-of-Concept-Tool namens `FrontRange DSM Password Decryptor`, das in der Lage ist, alle Passwortinformationen zu entschlüsseln, die in den Konfigurationsdateien `NiCfgLcl.ncp` und `NiCfgSrv.ncp` gespeichert sind. Die folgende Ausgabe dieses Software-Tools (siehe Listing 1) zeigt eine erfolgreiche Passwortwiederherstellung.

Listing 1: Erfolgreiche Passwortwiederherstellung mit Hilfe des PoC-Software-Tools

```
>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!
```

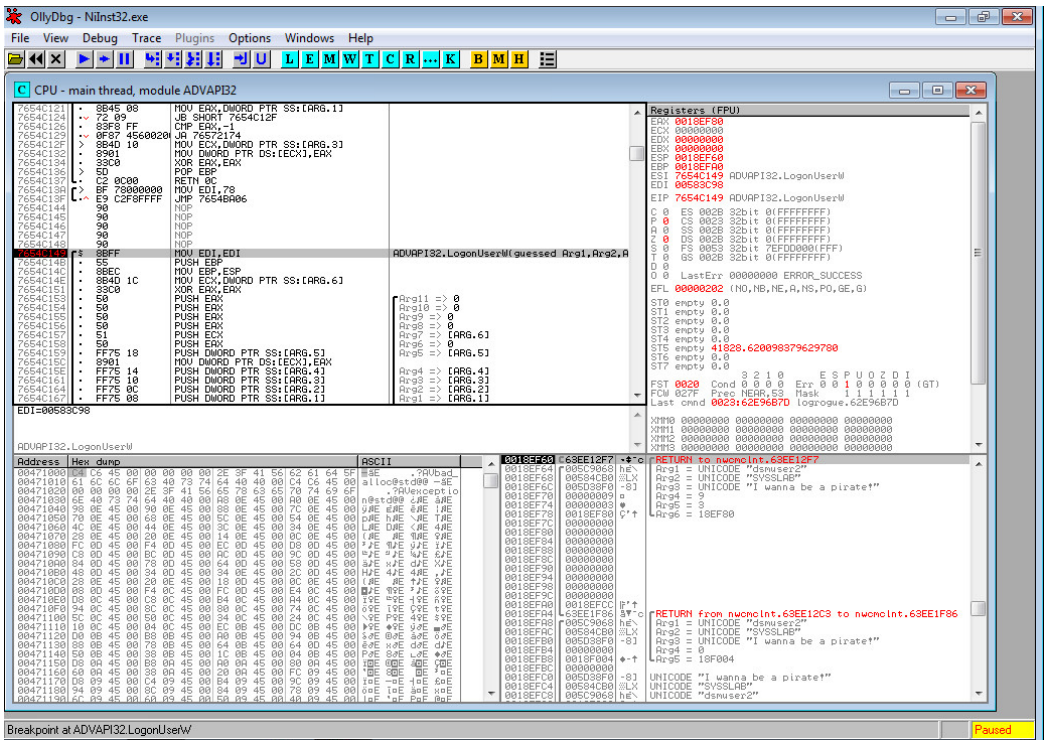

Abbildung 2: Auslesen des entschlüsselten Klartextpasswortes des FrontRange DSM-Benutzerkontos DSM Distribution Service aus dem Speicher des Prozesses NiInst32.exe mittels OllyDbg

Die beschriebenen Sicherheitsschwachstellen konnten in den folgenden FrontRange DSM Softwareversionen erfolgreich ausgenutzt werden:

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

Fazit

Die Softwarelösung FrontRange DSM schützt sensible Anmeldedaten unzureichend und verletzt Designprinzipien der sicheren Softwareentwicklung. Eingeschränkte Benutzerkonten haben lesenden Zugriff auf die gespeicherten Passwortinformationen, die Passwörter können mit einem statischen kryptografischen Schlüssel im Klartext wiederhergestellt werden. Aufgrund des Softwaredesigns werden die Passwörter zudem im Kontext eines niedrigprivilegiertern Benutzerprozesses (`NiInst32.exe`) verwendet, der durch einen Angreifer oder eine Schadsoftware im selben niedrigprivilegierten Benutzerkontext analysiert und kontrolliert werden kann.

Die SySS GmbH bewertet die gefundenen Schwachstellen als hohes Sicherheitsrisiko, da sie bei Angriffen zur Rechteausweitung genutzt werden können, die sogar in administrativen Berechtigungen für gesamte Windows-Domänen resultieren 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 und niedrigprivilegierte Benutzerprozesse ein äußerst ungeeigneter Ort, um sie zu verwenden.

Eine ähnliche Schwachstelle, die die Softwarekomponente McAfee Security Agent der Antivirensoftware McAfee VirusScan Enterprise betrifft, wurde in der SySS-Publikation *Rechteausweitung mittels Antivirensoftware* [4] aus dem Jahr 2011 beschrieben. Eine weitere populäre Sicherheitsschwachstelle dieser Art betrifft das Setzen von Passwörtern unter Verwendung von Group Policy Preferences (GPP) mit Microsoft Windows Server-Betriebssystemen, die ebenfalls für Angriffe zur Rechteausweitung genutzt werden können [5].

Die SySS GmbH empfiehlt, das Softwaredesign der Client-Management-Software FrontRange DSM zu ändern, sodass sensible Passwortinformationen nur bestimmten hochprivilegierten Benutzerkonten zugänglich sind und auch nur von diesen verarbeitet werden, wie beispielsweise Windows-Dienstkonten mit SYSTEM-Rechten. Auf diese Weise ist ein niedrigprivilegierter Angreifer oder eine Schadsoftware nicht in der Lage, auf sensible Passwortinformationen zuzugreifen, um diese wiederherzustellen.

Der Softwarehersteller FrontRange USA Inc. wurde von der SySS GmbH über die gefundenen Sicherheitsprobleme mit dem Security Advisory SYSS-2014-007 [6] in Kenntnis gesetzt. Nach Informationen von FrontRange wurden die beschriebenen Schwachstellen in einer neuen Softwareversion behoben, die ab dem 30. April 2015 verfügbar ist. Für weitere Informationen oder Support wenden Sie sich bitte an den Hersteller FrontRange.

Referenzen

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

[2] FrontRange DSM Getting Started Guide

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

[4] Matthias Deeg und Sebastian Schreiber, *Rechteausweitung mittels Antivirensoftware,* https://www.syss.de/fileadmin/ressources/040_veroeffentlichungen/dokumente/Rechteausweitung_mittels_Antivirensoftware.pdf

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

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