Matthias Deeg

Rechteausweitung mittels Client-Management-Software – Teil II

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

Erst kürzlich veröffentlichte die SySS GmbH ein Security Advisory und einen Artikel über Schwachstellen bezüglich der Verwaltung von Anmeldedaten in der Client-Management-Software FrontRange DSM, die erfolgreich für Angriffe zur Rechteausweitung ausgenutzt werden konnten, was häufig in administrativen Berechtigungen für gesamte Windows-Domänen resultierte [1], [2].

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 und 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.

Die Client-Management-Software Empirum des Herstellers Matrix42 [3] und insbesondere deren Komponente Empirum Inventory war in der Vergangenheit und ist heute noch eines dieser interessanten und lohnenswerten Ziele aus der Perspektive eines Angreifers, da sie sensible Anmeldedaten unzureichend schützt und Designprinzipien der sicheren Softwareentwicklung verletzt.

Diese Schwachstellen in der Verwaltung von Anmeldedaten der Empirum Client-Management-Software sind nicht neu und wurden seit 2009 regelmäßig und erfolgreich bei Sicherheitstests von der SySS GmbH und sehr wahrscheinlich auch von vielen anderen Angreifern, sowohl mit guten als auch mit bösen Absichten, für Rechteausweitungen ausgenutzt, die oftmals in administrativen Berechtigungen für gesamte Windows-Domänen resultierten. Nach Informationen der SySS GmbH sind diese Sicherheitsschwachstellen dem Softwarehersteller Matrix42 seit mindestens Ende 2009 bekannt. Des Weiteren wurden diese Sicherheitsschwächen unabhängig vor mehr als drei Jahren durch den Autor otr gemeldet und in einem Security Advisory am 14. Februar 2013 über die Full Disclosure Mailing-Liste veröffentlicht [4]. Dennoch sind diese Sicherheitsschwachstellen heute im Jahr 2015 immer noch präsent und können noch genauso erfolgreich ausgenutzt werden wie 2009.

Sicherheitsanalyse

Im Rahmen eines Sicherheitstests eines Client-Systems, das mit der Client-Manage-

ment-Software Empirum verwaltet wurde, stellte die SySS GmbH fest, dass die Softwarekomponente Empirum Inventory sensible Anmeldedaten auf unsichere Weise speichert und verwendet. Dadurch wird ein Angreifer oder Schadsoftware mit Dateisystemzugriff auf ein verwaltetes Client-System oder auf bestimmte Empirum-Netzlaufwerke, beispielsweise mit den Berechtigungen eines eingeschränkten Windows-Benutzers, in die Lage versetzt, die Klartextpasswörter einer oder mehrerer konfigurierter Empirum-Benutzerkonten wiederherstellen zu können.

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 normalerweise mindestens ein Benutzerkonto von Empirum lokale administrative Berechtigungen auf verwalteten Computersystemen benötigt.

Empirum unterstützt die folgenden vier Passwortformate, um Passwortinformationen in verschlüsselter Form in unterschiedlichen Konfigurationsdateien oder in der Windows-Registry zu speichern:

1. SETUP
   Beispiel: `*SKZjk`&gp2`
2. SYNC
   Beispiel: `12B65B9A30D4237D0A5F8D50341581B64207CE74CDE2ED76328D55EDE775EF4A71631812F2E4E39BD951E26991F307F`
3. EIS
   Beispiel: `A"z!' |-%-*),$ „!&(xiYJ|+./'(=&)+#$,#%./*X`
4. MD5
   Beispiel: `8a24367a1f46c141048752f2d5bbd14b`

Die Empirum-Passwortformate SETUP, SYNC und EIS nutzen umkehrbare kryptografische Methoden und können mit Hilfe eines Software-Tools namens `EmpCrypt.exe` erzeugt werden. Für gewöhnlich haben nur Empirum-Administratoren Zugriff auf dieses Software-Tool und es ist nicht auf verwalteten Systemen installiert. Aber Empirum-Softwarekomponenten wie Empirum Inventory und deren Module (beispielsweise `EmpInventory.exe`, `ShowInventory.exe`), die auf verwalteten Computersystemen installiert sind, beinhalten die Funktionalität für das Entschlüsseln dieser Empirum-Passwortformate. Die verwendeten MD5-Passwörter sind einfach *ungesalzene* MD5-Hash-Werte des Klartextpassworts.

Konfigurationsdateien mit verschlüsselten Passwortinformationen in Form von SETUP, SYNC, EIS oder MD5-Passwörtern befinden sich entweder auf den verwalteten Systemen selbst, beispielsweise in der Konfigurationsdatei `AgentConfig.xml`, oder in INI-Dateien, die auf Netzfreigaben von Empirum-Servern gespeichert sind.

Ein Windows-Domänenbenutzer mit eingeschränkten Berechtigungen hat lesenden Zugriff auf die lokal gespeicherte XML-Konfigurationsdatei und auf die INI-Konfigurationsdateien, die für gewöhnlich an den folgenden Orten gespeichert sind:

- `\\<EMPIRUM SERVER>\Configurator$`
- `\\<EMPIRUM SERVER>\Values$`

Eine Analyse der verwendeten Verschlüsselungsmethoden für SETUP-, SYNC- und EIS-Passwörter von Empirum durch die SySS GmbH ergab, dass drei unterschiedliche Verschlüsselungsmethoden verwendet werden, jede mit ihrem eigenen statischen (*hard-coded*) Geheimnis (zum Beispiel ein kryptografischer Schlüssel oder eine Permutationstabelle).

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

Ein solcher Online-Angriff, der den laufenden Prozess `EmpInventory.exe` zum Ziel hat, kann beispielsweise mit Hilfe eines Softwaredebuggers wie OllyDbg [5] aus der Perspektive eines eingeschränkten Windows-Benutzers durchgeführt werden.

Ein anderer Weg für einen Angreifer oder Schadsoftware mit Dateisystemzugriff auf Konfigurations-

dateien von Empirum 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 bei den verschiedenen Empirum-Passwortformaten SETUP, SYNC und EIS tatsächlich verschlüsselt werden. Ein Angreifer mit Dateisystemzugriff auf das Zielsystem kann (un)glücklicherweise die clientseitigen Komponenten der Client-Management-Software Empirum analysieren, wie etwa die ausführbare Datei `EmpInventory.exe` oder andere relevante Programmbibliotheken (DLLs), wie beispielsweise `Cryptography.dll`, und die Funktionsweise der Verschlüsselungsmethoden herausfinden.

Mit diesem Wissen können alle gespeicherten SETUP-, SYNC- und EIS-Passwörter von Empirum augenblicklich im Klartext wiederhergestellt werden.

Die SySS GmbH entwickelte ein Proof-of-Concept-Tool namens `Empirum Password Decryptor` für Windows und Linux, das in der Lage ist, SETUP-, SYNC- und EIS-Passwörter zu entschlüsseln.

Die folgenden drei Ausgaben dieses Software-Tools zeigen beispielhaft erfolgreiche Passwortwiederherstellungen von verschlüsselten SETUP-, SYNC- und EIS-Passwörtern (siehe grauer Kasten).

Die beschriebenen Sicherheitsschwachstellen konnten in den folgenden Softwareversionen von Empirum erfolgreich ausgenutzt werden:

- `v14.2.1`
- `v15.1.0`

Wie in dem Security Advisory *Empirum Password Obfuscation Design Flaw* [4] beschrieben, kann das Software-Tool `EmpCrypt.exe` auf einfache Weise durch die Modifikation eines bedingten Sprungbefehls (*conditional jump*) so manipuliert werden, dass es für die Entschlüsselung von Empirum-Passwörtern in den Formaten SETUP, SYNC und EIS genutzt werden kann. Falls ein Angreifer Zugriff auf das Software-Tool `EmpCrypt.exe` besitzt, so kann er Empirum-Passwörter unverzüglich mit minimalem Aufwand und ohne zeitaufwändige Code-Analysen im Klartext wiederherstellen. Natürlich gilt dies auch, falls ein Angreifer Zugriff auf ein Software-Tool wie `Empirum Password Decryptor` haben sollte.

```
$ ./epd ,*SKZjk`&gp2‘

____ ___  ___
|___ |__] |  \
|___ |    |__/
Empirum Password Decryptor v2.0 by Matthias Deeg - SySS GmbH (c) 2009-2015
[*] Read Empirum SETUP password
[+] The decrypted password is: P@ssw0rd!


$ ./epd 12B65B9A30D4237D0A5F8D50341581B64207CE74CDE2ED7632D8D55EDE775EF4A-
71631812F2E4E39BD951E26991F307F

____ ___  ___
|___ |__] |  \
|___ |    |__/
Empirum Password Decryptor v2.0 by Matthias Deeg - SySS GmbH (c) 2009-2015
[*] Read Empirum SYNC password
[+] The decrypted password is: P@ssw0rd!


E:\>epd.exe „A\"z!‘ ^|-%-*),$ \"!&(xiYJ|+./‘(=&)+#$,#%./*X"

____ ___  ___
|___ |__] |  \
|___ |    |__/
Empirum Password Decryptor v2.0 by Matthias Deeg - SySS GmbH (c) 2009-2015
[*] Read Empirum EIS password
[+] The decrypted password is: P@ssw0rd!
```

Die SySS GmbH wird das entwickelte Software-Tool `Empirum Password Decryptor` nicht veröffentlichen.

Fazit

Die Client-Management-Softwarelösung Empirum schützt sensible Anmeldedaten unzureichend und verletzt Designprinzipien der sicheren Softwareentwicklung. Eingeschränkte Benutzerkonten haben lesenden Zugriff auf die gespeicherten Passwortinformationen, die Passwörter in den Empirum-Passwortformaten SETUP, SYNC und EIS können mit statischen Geheimnissen (zum Beispiel ein kryptografischer Schlüssel oder eine Permutationstabelle) im Klartext wiederhergestellt werden. Aufgrund des Softwaredesigns werden die Passwörter zudem im Kontext eines niedrigprivilegierten Benutzerprozesses (`EmpInventory.exe`) verwendet, der durch einen Angreifer oder 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.

Generell sollte der Zugriff auf Passwortinformationen, auch wenn diese verschlüsselt sind, 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 Client-Management-Software FrontRange DSM betrifft, wurde in unserer SySS-Publikation *Rechteausweitung mittels Client-Management-Software* [2] 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 [6].

Die SySS GmbH empfiehlt dem Softwarehersteller Matrix42, das Softwaredesign der Client-Management-Software Empirum 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 Schadsoftware nicht in der Lage, auf sensible Passwortinformationen zuzugreifen, um diese wiederherzustellen.

Aktuell ist der SySS GmbH keine Lösung für die beschriebenen Sicherheitsschwächen bekannt. Falls Sie die Client-Management-Software Empirum nutzen und möglicherweise von diesen Schwachstellen betroffen sein sollten, wenden Sie sich bitte an den Softwarehersteller Matrix42 für weitere Informationen.

Referenzen

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

[2] Matthias Deeg, *Rechteausweitung mittels Client-Management-Software,* https://www.syss.de/fileadmin/dokumente/Publikationen/2015/Rechteausweitung_mittels_Client-Management-Software.pdf

[3] Matrix42 Webseite, https://www.matrix42.com/de/

[4] Full Disclosure Mailing List, Empirum Password Obfuscation Design Flaw, http://seclists.org/fulldisclosure/2013/Feb/71

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

[6] 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