Matthias Deeg

Privilege Escalation via Client Management Software – Part II

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

Recently, the SySS GmbH published a security advisory and an article about vulnerabilities concerning the credentials management of the client management software FrontRange DSM that could be successfully exploited in privilege escalation attacks resulting in administrative privileges for entire Windows domains [1], [2].

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, and 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.

The client management software Empirum from Matrix42 [3] and especially its component Empirum Inventory has been, and still is, one of these interesting and rewarding targets from an attacker‘s perspective, because it insufficiently protects sensitive user credentials and violates secure design principles.

These vulnerabilities concerning the Empirum credentials management are not new and have been regularly and successfully exploited by the SySS GmbH since 2009 during security assessments and most probably also by many other attackers, either with good or bad intentions, in privilege escalation attacks that often resulted in administrative privileges for entire Windows domains. According to information of the SySS GmbH, the manufacturer Matrix42 knows about these security issues at least since the end of 2009. Furthermore, these vulnerabilities were independently reported and publicly disclosed more than three years ago on February 14, 2013, in a security advisory by the author otr on the Full Disclosure mailing list [4]. However, these Empirum security vulnerabilities are still present today in 2015 and can be successfully exploited just like in 2009.

Security Assessment

During a security assessment of a client system managed with Empirum, the SySS GmbH found out that the software component Empirum Inventory stores and uses sensitive user credentials in an insecure manner. This enables an attacker or malware with file system access to a managed client or to specific Empirum network shares, for example with the privileges of a limited Windows domain user account, to recover cleartext passwords of one or more configured Empirum user accounts.

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 usually at least one Empirum user account needs local administrative privileges on managed systems.

Empirum supports the following four password formats for storing password information in an encrypted way in different configuration files or in the Windows registry:

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

The Empirum SETUP, SYNC, and EIS password formats use reversible encryption methods and can be created by a software tool called EmpCrypt.exe. Usually, only Empirum administrators have access to this software tool and it is not installed on managed systems. But Empirum software components like Empirum Inventory and its modules (for example EmpInventory.exe, ShowInventory.exe) that are installed on managed systems contain the functionality for decrypting these Empirum password formats. The used MD5 passwords are simply unsalted raw MD5 hashes.

Configuration files containing encrypted password information in the form of SETUP, SYNC, EIS, or MD5 passwords are either located on the managed system itself, for example in the configuration file AgentConfig.xml, or in INI files stored on network shares of Empirum servers.

A limited Windows domain user has read access to the locally stored XML configuration file and to the INI configuration files that are usually stored in the following locations:

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

An analysis of the used encryption methods for Empirum SETUP, SYNC, and EIS passwords by the SySS GmbH showed, that three different encryption algorithms are used, each with its own hard-coded secret (for example a cryptographic key or permutation table).

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

For instance, such an online attack targeting the running process EmpInventory.exe can be performed using an application-level debugger like OllyDbg [5] from the perspective of a limited Windows user.

Another way for an attacker or malware having file system access to Empirum 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 using the different Empirum password formats SETUP, SYNC, and EIS are actually encrypted. Fortunately, by having file system access to the target system, an attacker can analyze the client-side components of the client management software Empirum, like the executable file EmpInventory.exe or other relevant dynamic link libraries (DLLs) like Cryptography.dll, and find out how the encryption is done.

With this gained knowledge all stored Empirum SETUP, SYNC, and EIS passwords can be instantly recovered as cleartext.

The SySS GmbH developed a proof-of-concept software tool named Empirum Password Decryptor for Windows and Linux which is able to decrypt Empirum SETUP, SYNC, and EIS passwords.

The following three outputs of this software tool exemplarily show successful password recoveries of Empirum SETUP, SYNC, and EIS passwords (see grey box).

The described security vulnerabilities concerning the credentials management could be successfully exploited with the following Empirum software versions:

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

As described in the security advisory *Empirum Password Obfuscation Design Flaw* [4], the software tool `EmpCrypt.exe` can easily be patched by modifying a conditional jump instruction in order decrypt Empirum SETUP, SYNC, and EIS passwords. Thus, if an attacker has access to the software tool `EmpCrypt.exe`, she will be able to recover Empirum cleartext passwords instantly with minimal effort without the need of time-consuming code analyses. Of course, the same is true if an attacker has access to a software tool like `Empirum Password Decryptor`. The SySS GmbH will not publicly disclose the developed software tool `Empirum Password Decryptor`.

Conclusion

The client management software solution Empirum insufficiently protects sensitive user credentials and violates secure design principles. Limited user accounts have read access to the stored password information, the Empirum SETUP, SYNC, and EIS passwords can be recovered as cleartext using hard-coded secrets (for example a cryptographic key or permutation table), and due to the software design, the passwords are also used in the context of a low-privileged user process (`EmpInventory.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

```
$ ./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!
```

to store such data, and low-privileged user processes are not the proper place to use them.

A similar security vulnerability affecting the client management software FrontRange DSM has been described in our paper *Privilege Escalation via Client Management Software* [2]. 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 [6].

The SySS GmbH recommends the manufacturer Matrix42 to change the software design of the client management software Empirum, 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.

Currently, the SySS GmbH is not aware of a solution for the described security issues. If you are using the Empirum client management software and are possibly affected by the these security vulnerabilities, please contact the manufacturer Matrix42 for further information.

References

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

[2] Matthias Deeg, *Privilege Escalation via Client Management Software,* https://www.syss.de/fileadmin/dokumente/Publikationen/2015/Privilege_Escalation_via_Client_Management_Software.pdf

[3] Matrix42 Website, https://www.matrix42.com/en/

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

[5] OllyDbg Website, 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