EMPIRUM VULNERABILITIES

The Empirum Client Management Software is used for typical client management tasks, such as

- Inventory and asset management
- Patch Management
- Software Management
- License Management

According to Matrix42, over 5000 customers worldwide use the client management software.[1] The large amount of big companies using the software makes Matrix42 one of the market leaders in the field of client management software. A critical vulnerability in this software affects many large companies worldwide.

as Already in 2009, a vulnerability in the Empirum client management software was discovered which made it possible to decrypt passwords. [2] The vulnerability allowed a local attacker or malicious software with read access to the file system of a client or an Empirum Software Server network share, to decrypt obfuscated service account passwords stored in configuration files. This vulnerability could be exploited using the file `Empcrypt.exe`. This file is actually used to obfuscate passwords, but could be used to deobfuscate the passwords by patching the binary. This vulnerability has been fixed after several years by modifying `Empcrypt.exe`.

The Empirum Client Management Software uses four algorithms for password obfuscation or encryption:

- EIS (in-house development)
- SETUP (in-house development)
- SYNC (in-house development)
- AES256

For the obfuscation algorithms EIS and SETUP, r-tec IT Security GmbH was able to find new vulnerabilities. These vulnerabilities are not, as before, based on binary patching the `Empcrypt.exe` file, but on problems with the obfuscation algorithms themselves.

- The vulnerability in EIS allows decryption of obfuscated passwords (CVE-2019-16259);
- The vulnerability in SETUP allows to infer password metadata (CVE-2019-162260)

Since the discovery of the vulnerabilities, r-tec has been able to exploit them in many different company environments using the Empirum Client Management Software. Through this, an estimation of the potential risk can be determined. In quite a half of the cases, this vulnerability could be used to increase rights up to domain administrator rights or at minimum client administrator rights. It should be noted, however, that access to the `Empcrypt.exe` is still required to exploit the vulnerability, making this process more difficult.

[1] https://www.matrix42.com/en/customers/
[2] https://www.syss.de/fileadmin/dokumente/Publikationen/2015/Rechteausweitung_mittels_Client_Management_Software__Teil_II.pdf

CVE-2019-16259

The EIS obfuscated passwords are located in .INI files, which can be found on the client as well as in network shares of the Empirum server:

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

The EIS-obfuscated passwords start with the ASCII character "A" and end with the character "X". Between these two characters is the obfuscated password itself. The `EmpCrypt.exe` always generates the same obfuscated string using the EIS algorithm for the same plaintexts. This allows attackers with access to the `Empcrypt.exe` to obfuscate large wordlists to obtain all possible resulting obfuscated passwords. When accessing an .INI configuration file, the attacker can look in the list of obfuscated passwords for comparison. If the same value is found, the attacker already knows the cleartext password. The string "P@ssw0rd! " for example results in the following obfuscated password:

```
A"z!' |-%-*),$ "!&(xiYJ|+./'(=&)+#$,#%./*X
```

r-tec found out by generating many different obfuscated passwords using `Empcrypt.exe` that there is a one-to-one correspondence between plaintext characters and obfuscated characters. For example, the first character of a plaintext always corresponds to the 21st character of the obfuscated password. The capital letter "P" has thus become a capital "Y". The exact assignment of plaintext to obfuscated text is as follows

```
$decryptSequence = 21,22,19,2,6,29,23,20,24,12,9,25,26,14,3,15,33,
  34,37,30,27,28,31,10,32,35,7,38,39,5,16,1,36,13,8,17,4,18,11,40
```

The first character of the plain-text password corresponds to the 21st character of the obfuscated password, the second character to the 22nd character, the third to the 19th character, and so on. With the knowledge of this one-to-one mapping, an attacker is able to decrypt EIS-obfuscated passwords. The only required dependency is access to the `Empcrypt.exe` as well as `Matrix42.Common.AppVerificator.dll`. The decryption process is as follows:To obtain the first plaintext password character, the attacker encrypts each character of the ASCII table using `Empcrypt.exe` and compares the 21st character of the resulting obfuscated password with the obfuscated passwords 21th charackter from the configuration file. If the 21st character matches, the first plain-text password character is found. To obtain the second plain-text password character, the attacker generates all possible ASCII characters again, but precedes the first character already known. If the 22nd digit of the obfuscated password matches the one in the configuration file, the second plaintext password character is found. In this way a complete decryption of any EIS obfuscated password is possible. To simplify these steps, r-tec has written software to automate this process:

Figure 1: Automatic de-obfuscation of EIS passwords

The POC code to exploit this vulnerability can be obtained from the following GIT repository:

`https://github.com/S3cur3Th1sSh1t/EmpEISDecrypt`

A further finding of the analyses was that the EIS password, which was used as an example for the vulnerabilities already found in 2009, can still be de-obfuscated in the same way today and produces the same cleartext. Conversely, this means that any attacker who tapped the unpatched `Empcrypt.exe` in a company in the period 2009 - 2015 can still decrypt any password of any algorithm today. The three in-house algorithms have not changed for over ten years.

This way of decrypting passwords was shown to Matrix42 in a presentation. According to the manufacturer, the following workarounds should be applied to make it more difficult for attackers to access the .INI files:

1) By installing the latest Empirum Agent version 18.0.2 or higher, access to the .INI files on a client is restricted to administrative users. By this measure, the EIS passwords can only be read by administrative users.
2) The permissions of the Empirum Server network shares should be adjusted so that not every user in the domain gets access, but only a very limited circle of users.
3) The storage of highly privileged user account passwords in the configuration files should be avoided.
4) Implementation of the QuickSync feature, distributing the .INI files to only a few servers.

According to Matrix42, all obfuscation algorithms will be replaced by AES encryption in the future.

From r-tec's experience, various companies allow access to the Empirum Server network shares for each domain user. This allows every user in the domain to access and decrypt all the passwords.

CVE-2019-16260

The SETUP obfuscated passwords are located in the same configuration files as the EIS passwords. For this algorithm, r-tec was able to identify vulnerabilities that can be used to obtain metadata for the plain-text passwords used. For example, the length of a password can be determined directly on read access to the obfuscated password:

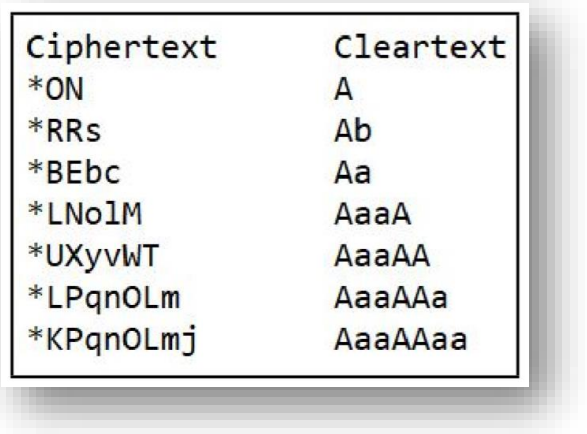
Ciphertext	Cleartext
*G (Empty)	
*QP	(A)
*KMJ	(AA)
*DGDE	(AAA)
*AEBC@	(AAAA)
*UXYVWT	(AAAAA)
*HLMJKHI	(AAAAAA)
*EJKHIFGD	(AAAAAAA)
*HNOLMJKHI	(AAAAAAAA)
*QXYVWTURSP	(AAAAAAAAA)
*OYVWTURSPQN	(AAAAAAAAAA)
*LWTURSPQNOLM	(AAAAAAAAAAA)
*FPQNOLMJKHIFG	(AAAAAAAAAAAA)
*BOLMJKHIFGDEBC	(AAAAAAAAAAAAA)
*FRSPQNOLMJKHIFG	(AAAAAAAAAAAAAA)
*IVWTURSPQNOLMJKH	(AAAAAAAAAAAAAAA)
*CSPQNOLMJKHIFGDEB	(AAAAAAAAAAAAAAAA)
*CRSPQNOLMJKHIFGDEB	(AAAAAAAAAAAAAAAAA)
*FVWTURSPQNOLMJKHIFG	(AAAAAAAAAAAAAAAAAA)
*GXYVWTURSPQNOLMJKHIF	(AAAAAAAAAAAAAAAAAAA)
*FXYVWTURSPQNOLMJKHIFG	(AAAAAAAAAAAAAAAAAAAA)
*EXYVWTURSPQNOLMJKHIFGD	(AAAAAAAAAAAAAAAAAAAAA)
*DXYVWTURSPQNOLMJKHIFGDE	(AAAAAAAAAAAAAAAAAAAAAA)
*BYVWTURSPQNOLMJKHIFGDEBC	(AAAAAAAAAAAAAAAAAAAAAAA)
*BXYVWTURSPQNOLMJKHIFGDEBC	(AAAAAAAAAAAAAAAAAAAAAAAA)
*AXYVWTURSPQNOLMJKHIFGDEBC@	(AAAAAAAAAAAAAAAAAAAAAAAAA)

Figure 2: Changing the obfuscated password when changing the password length

A password with only one character always results in a SETUP-obfuscated password of two characters. Suppose an attacker finds the following SETUP password:

```
*KMJARA
```

With current knowledge, the length of the plain-text password here is five characters long. As long as there are no special characters or numbers in a password, an attacker can also deduce with high probability the number of upper and lower case letters present:



Ciphertext	Cleartext
*ON	A
*RRs	Ab
*BEbc	Aa
*LNolM	AaaA
*UXyvWT	AaaAA
*LPqnOLm	AaaAAa
*KPqnOLmj	AaaAAaa

Figure 3: Recognition Number of upper and lower case letters

However, this finding is not as reliable as the password length, as there are certainly deviations here:

Ciphertext	Cleartext
*GIe	Ab
*MNln	Abc
*QUqqU	AbcD
*PUqqUU	AbcDE
*GMiiMM6	AbcDE1
*MRprTJ?8	AbcDE15
*NTvpVT!:?	AbcDE151
*ELnhNL9277	AbcDE1512
*LTvpVT!:??8	AbcDE15124
*CLnhNL92770b	AbcDE15124a
*EQmmII:?8:3gS	AbcDE15124aV

Figure 4: Metadata deviations

For both the SETUP algorithm and the SYNC algorithm a randomization of the obfuscated password is performed. The same plaintext does not always result in the same obfuscated password. r-tec found out during further analyses that this randomization is carried out using the OS system time. If the system time is kept constant, e.g. using a batch script, no further randomization of the passwords takes place:

```
19:34:30,01>EmpCrypt.exe /S /SETUP "Fixed_time?"
*VFvfxxDnpur)

19:34:30,01>EmpCrypt.exe /S /SETUP "Fixed_time?"
*VFvfxxDnpur)

19:34:30,01>EmpCrypt.exe /S /SETUP "Fixed_time?"
*VFvfxxDnpur)

19:34:30,01>EmpCrypt.exe /S /SETUP "Fixed_time?"
*VFvfxxDnpur)

19:34:30,01>EmpCrypt.exe /S /SETUP "Fixed_time?"
*VFvfxxDnpur)
```

Figure 5: Generation of the same obfuscated password at the same system time

Since the .INI configuration files always contain a timestamp of the generation, SETUP as well as SYNC word list attacks can also occur for the algorithms SETUP as well as SYNC word list attacks analogous to the EIS algorithm. The attacker only has to reset the system time to that of the generation of the .INI file.