CVE, INNOVERY, RESEARCH

Bettini S.r.l. – SGSetup Hard-coded SSH private key

By Offensive Security Team @ Innovery Group S.p.A. | Febbraio 17, 2022

The Issue

The SGSetup software from Bettini S.r.l. is a software which allows to manage and configure the video surveillance system remotely.

It performs the same function as the web interface with the additional possibility of stopping the video stream of the cameras and modifying their configurations.
Upon connecting with the DVR/NVR device, the client initiates an SSH connection in order to

download configuration files from the remote device without asking for SSH username and password. Further investigations highlighted the presence of hard-coded private key inside the client itself.

Bettini promptly solved the problem with a new firmware release.

Who is impacted

GAMS product line devices which use SGSetup

Affected version

SGSetup prior to v.4.4.0

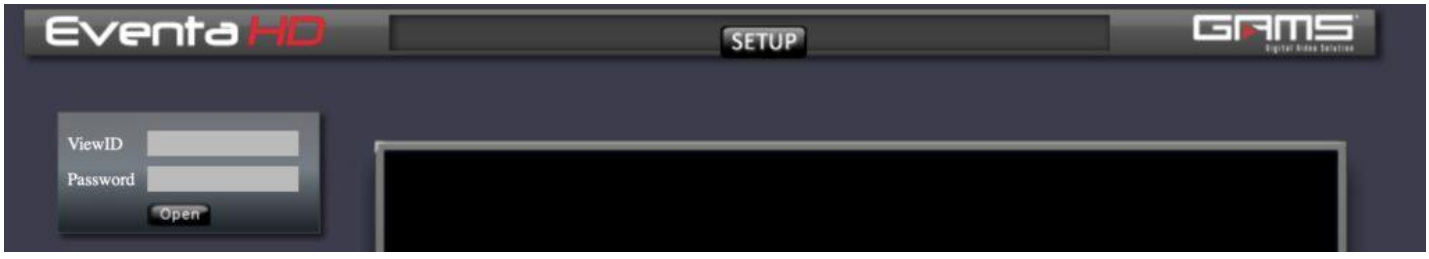
Mitigation

Update the firmware.

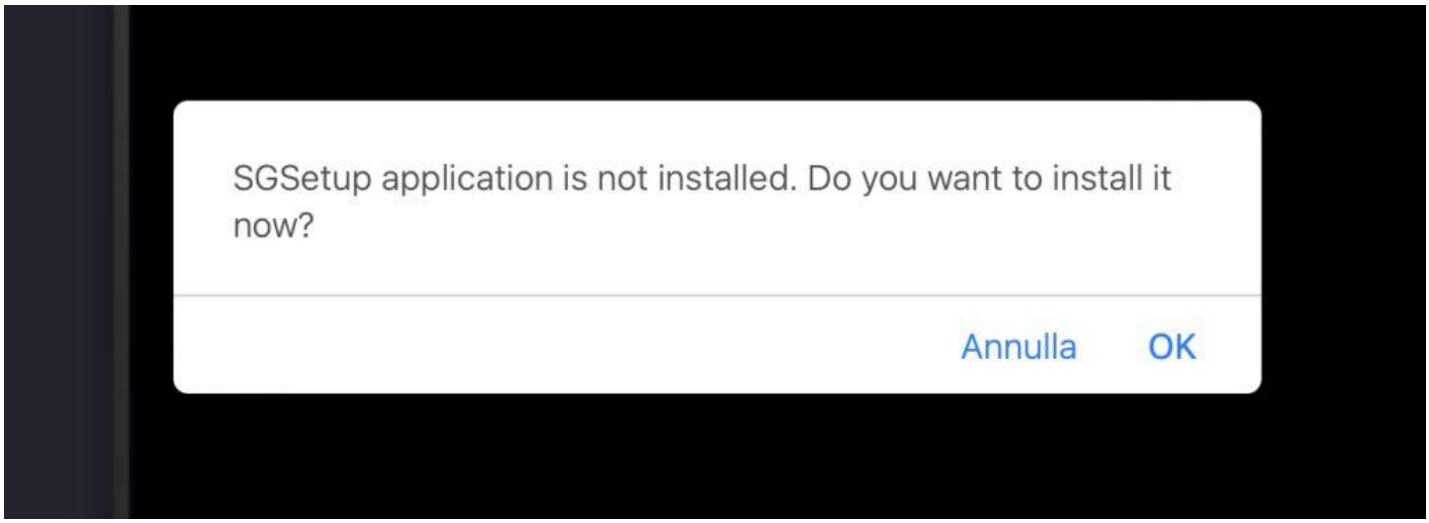
Do not expose the DVR/NVR SSH and web interface in the internet.

Exploitation

The devices web interface allows the download of SGSetup tool:

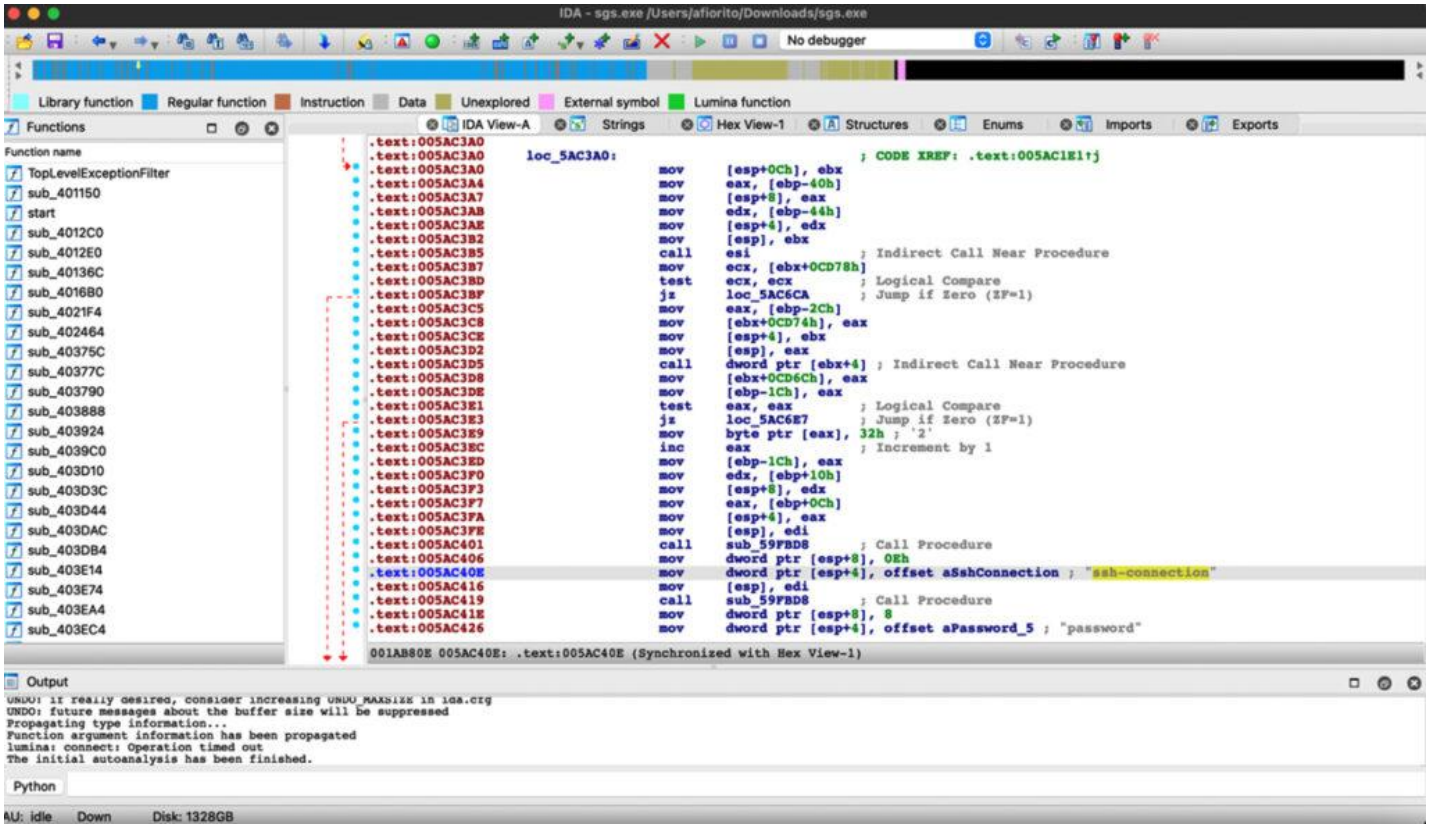


SGSetup Download #1



SGSetup Download #2

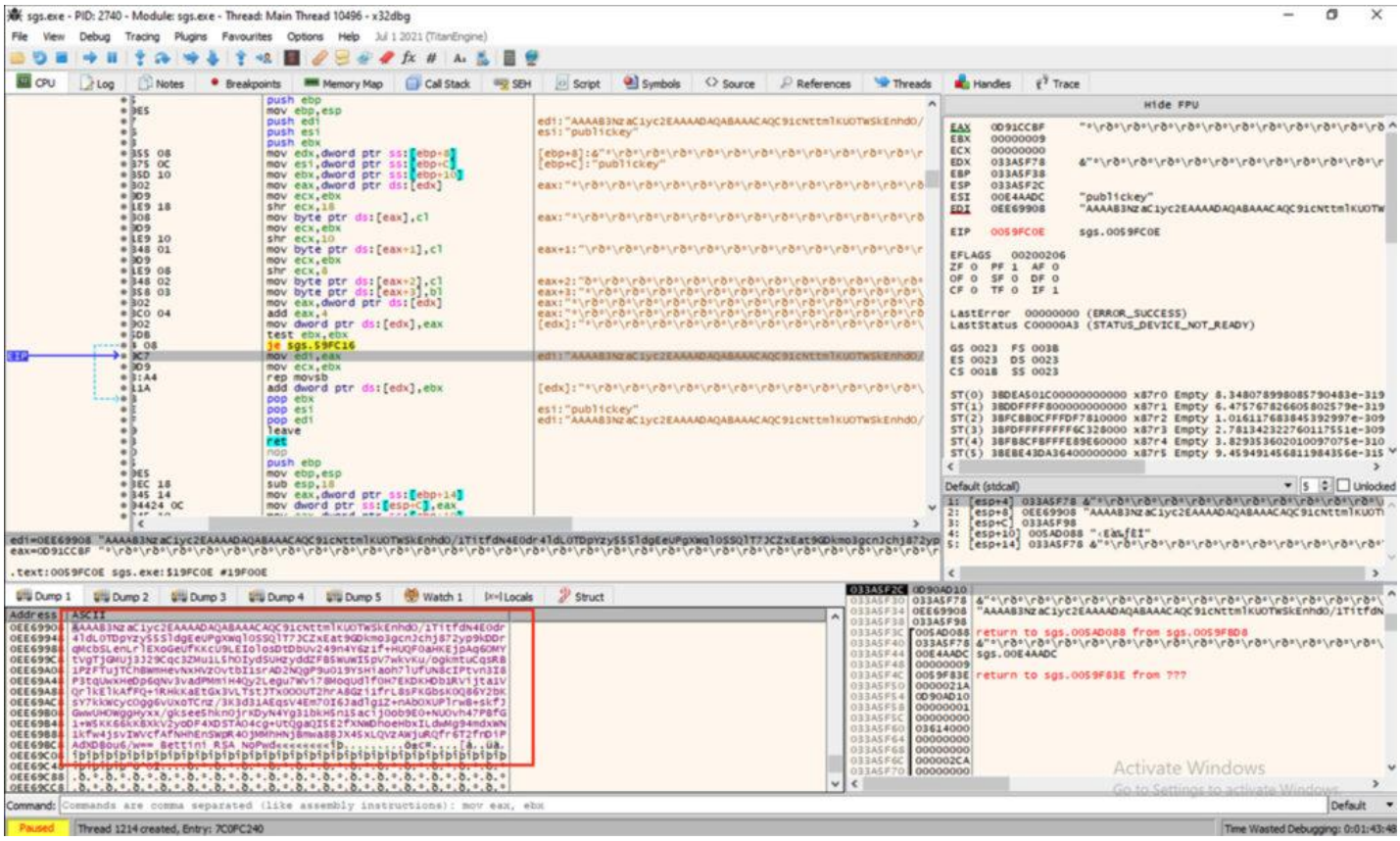
After a thorough reverse engineering process of the SGSetup software, the Innovery team was able to extract the RSA private key hard-coded inside the software.
The following image from the disassembler is showing all the low-level instructions executed by the software. It can be noted how the software tries to make an SSH connection.



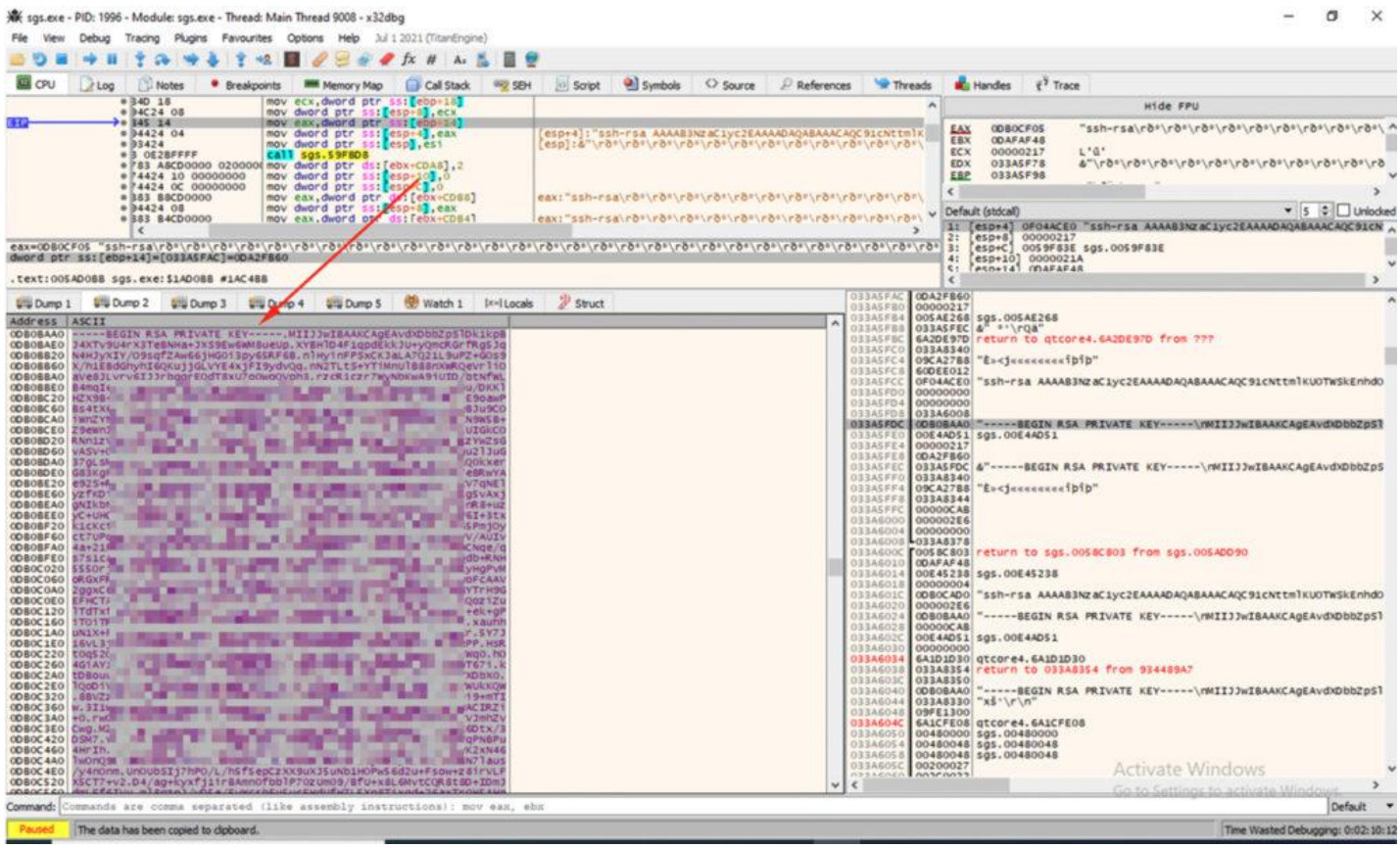
Disassembler

At this point the software was run with the help of a debugger in order to analyze each single instruction in real time. From the following image it is possible to see how the memory registers

were first allocated with the public key and then with the private key, object of interest, used to make the SSH connection:



Public Key



Private Key

The extracted key has been recomposed and formatted to be used to connect to the DVR as root user:

SSH Connection

The Team

- Antonio Fiorito
- Andrea Bruschi
- Francesco Petri
- Salvatore Volpes
- Jull Mendoza
- Fabio Villa
- Federico Zambito
- Gabriele Turcan

binary, CVE, debugger, hardcoded, ida, key, research, rsa, ssh

Kerberos Constrained Delegation

How to run notepad.exe with Powershell