SUPREMO Local privilege escalation

From: Adan Alvarez <adan.alvarez () a2secure com>
Date: Mon, 21 Dec 2020 17:00:58 +0100

```
Details
=======

Subject:  Local Privilege Escalation
Product: SUPREMO by Nanosystems S.r.l.
Vendor Homepage: https://www.supremocontrol.com/
Vendor Status: fixed version released
Vulnerable Version: 4.1.3.2348 (No other version was tested, but it is
believed for the older versions to be also vulnerable.)
Fixed Version: 4.2.0.2423
CVE Number: CVE-2020-25106
CVE URL:  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25106
Authors:  Víctor Gil (A2SECURE) Adan Alvarez (A2SECURE)

Vulnerability Description
=======

Allows attackers to obtain LocalSystem access because when running as a
service File Manager allows modifying files with system privileges. This
can be used by an adversary to, for example, rename Supremo.exe and then
upload a trojan horse with the Supremo.exe filename.

Proof of Concept
================

To exploit this vulnerability Supremo should be running as a service. Then
follow the following steps:

  - Connect to Supremo from a different machine.
  - Open File manager.
  - Go to the directory where the Supremo executable is located.
  - Modify the name of the executable.
  - Upload a malicious executable and rename it to Supremo.exe
  - Close supremo.

After these steps, as supremo is running as a service, the service
executes, as System, the executable allowing an attacker to elevate
privileges to System.

Fix
===

The vendor provides an updated version (4.2.0.2423)

 Timeline
========

2020-07-13 Disclosed to Vendor
2020-10-19 Vendor releases the final patch
2020-12-21 Advisory released

--
*Adan Álvarez*

Security Consultant

+34 933 945 600
aalvarez () a2secure com

--


*A2secure*

QSA auditors - Pentesting - Security Consultancy - Forensic
Analysis - PCI Consultancy - Malware Analysis - Incident Response -
Security Office - Security Training - Employee Security Awareness


Este
mensaje de correo electrónico y sus archivos adjuntos son confidenciales y
están legalmente protegidos. Se dirige exclusivamente al destinatario o
destinatarios. No está autorizado el acceso a este mensaje por otras
personas. Si Vd. no es la persona a la que va dirigido este email,
cualquier uso está prohibido y es ilegal. Asimismo, de acuerdo al
Reglamento EU 2016/679 sobre Protección de Datos Personales, le informamos
que su dirección e-mail forma parte de los ficheros de las empresas de
A2secure, S.L. (A2SECURE) con CIF: B65040107, porque en su momento nos
autorizó el tratamiento para mantener una relación comercial y/o
informativa de nuestros productos y servicios; Usted puede ejercer en
cualquier momento sus derechos de acceso, rectificación, supresión,
limitación y oposición dirigiéndose por escrito a Avda. Francesc Cambo 21,
10, 08003 Barcelona. Tel.: +34 93 3945600, Email: arco () a2secure com
<mailto:arco () a2secure com>. Si ha recibido este mensaje por error, por
favor, destrúyalo y notifíquelo. Gracias.


This message and its annexed
files may contain confidential information which is exclusively for the use
of the addressee. Access to this message by other people is not authorized.
If you are not the person to whom it is addressed, any use, treatment,
information, copy or distribution and any action or omission based on the
information contained in this message are strictly forbidden and illegal.
According to Regulation EU 2016/679 on Protection of Personal Data, we
inform you that your e-mail address is part of the files of the companies
of A2secure, S.L. (A2SECURE) with CIF: B65040107, because at some moment
you authorized us the treatment to maintain a commercial and / or
informative relationship of our products and services; You can exercise
your rights of access, rectification, erasure, restriction and object at
any time by writing to Avda. Francesc Cambo 21, 10, 08003 Barcelona. Tel .:
+34 93 3945600, Email: arco () a2secure com <mailto:arco () a2secure com>. If you
have received this message by mistake, please destroy it and notify it.
Thank you.
```

Current thread:

SUPREMO Local privilege escalation ***Adan Alvarez (Dec 21)***