SUPREMO 4.1.3.2348 Privilege Escalation

Authored by Victor Gil, Adan Alvarez

Posted Dec 22, 2020

SUPREMO version 4.1.3.2348 suffers from a privilege escalation vulnerability.

tags | exploit
advisories | CVE-2020-25106
SHA-256 | 692dd2b65bb1ca8014e4882531d9b3a1667493ce70b79b16343b0b5167f5bd2f

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
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:  Victor 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. Asímismo, 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.
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

packet storm

Site Links
- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us
- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By
- Rokasec

Follow us on Twitter

Subscribe to an RSS Feed