NetSetManPro 4.7.2 Privilege Escalation

Authored by Simon Bieber

Posted Jun 11, 2021

NetSetManPro version 4.7.2 suffers from a privilege escalation vulnerability.

tags | exploit
advisories | CVE-2021-34546
SHA-256 | e8a3f23fc7f163c05873cbfb945bc19268910c026e3331a239742efa41af0936 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Affected Products
    NetSetManPro 4.7.2 (other/older releases have not been tested)

References
    https://www.secuvera.de/advisories/secuvera-SA-2021-01.txt (used for
updates)
    CVE-2021-34546
(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34546)

Summary:
    "NetSetMan is a network settings manager software for easily
switching between
    your preconfigured profiles."

    The save file dialogue within the action log window after switching a
profile
    using the pre-logon profile switching (if intentionaly enabled) leads
to
    arbitrary command execution as system authority user enabling an
unauthenticated
    attacker to log on.

Effect:
    An unauthenticated attacker with physical access to a computer with
NetSetMan Pro
    4.7.2 installed, that has the pre-logon profile switch activated (not
enabled by
    default) as button withinthe windows logon screen, is able to drop to
an admin-
    istrative shell and execute arbitrary commands as system user by the
use of the
    "save log to file" feature within NetSetMan Pro.

Example:
    On a client computer running Microsoft Windows 10 and NetSetMan Pro
an Icon can
    appear on the Windows lock-screen if configured. The following steps
must be per-
    formed in order to gain an administrative shell:
    1. Boot the client system
    2. Click on the NetSetMan Pro Icon.
    3. Choose an user defined (empty) setting.
    4. Click on the "save" button in the appearing Window within the
"Log" section
       (save icon)
    5. Click on "File-Type" and Choose "*.*"
    6. Navigate to path "C:\Windows\System32\"
    7. Right-Click on on "cmd.exe" and choose "Run as administrator...".
    8. The appearing command prompt has administrative rights.

    To be able to bypass authentication a local user with administrative
rights can
    be added using the following commands:
    a. net user Pentest Password123! /add
    b. net localgroup Administrators Pentest /add

Solution:
    Update to Version 5.0 or newer (5.0.6 was tested by the researcher).

Disclosure Timeline:
    2021/05/17 vendor initially contacted, submitted all details.
    2021/05/17 vendor replied suggesting vulnerability already fixed
               in newer versions prior researcher contact
    2021/06/02 verified vendor suggested fix using version 5.0.6;
               updated advisory and contacted vendor again; vendor
               suggested edits
    2021/06/09 updated advisory and requested CVE identifier
    2021/06/10 public disclosure

Credits:
    Simon Bieber
    sbieber@secuvera.de
    secuvera GmbH
    https://www.secuvera.de

Disclaimer:
     All information is provided without warranty. The intent is to
     provide information to secure infrastructure and/or systems, not
     to be able to attack or damage. Therefore secuvera shall
     not be liable for any direct or indirect damages that might be
     caused by using this information.

This message is signed with my PGP key (Short Key ID 661263A5)
You can download it here:
https://www.secuvera.de/download/simon-bieber-short-key-id-661263a5/
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE6mgEBCu3JYBgmGrgDIJc8mYSY6UFAmDDFocACgkQDIJc8mYS
Y6V1YBAAivvBI79oAYKrkkELU1drnEtIloRggLF6PQ4BlBgZ1DMfLQLcbACVT2LY
ro9SBpU/s6AOaZ98jETA/nS57MD+70ncEevP6hm3DzxV1mHtS4rjTU6hkcFfC8tq
rqeXRz4tloWhPQd+AB2TOvpUIRtVn4zomNs9e3YkYRhRBixqZgrLz/c0mQjKIW/u
+hf0v5RYYSwA8q9LyhN6QUmm0UCVg06o5518+eyc6V1JeMekdX7ais99Ki/FNmYw
z66aP4FrPx+RpCVsl0sCpMiZWIhNtUVq37uNJCaE55K6li241RVDLmzZtNFThx8F
maqdUalwdEJ3AY8Ays/s2HWq4EkTyAlKey25NvSUVNUvYwqDgE/TzXK/rqVpIvIs
+dTiEJIQ8aBlRL61UF6ddz2f1lVj85q/4tQCJ/Nk062pkpI2bfhsgeEnvwkkQrTp
YqlnlzOR4THpWsiUQOq3VeFFDU33T8Lch1wpURNtRlVlO+Zx4T4W+UX5Q3uIfprF
04TwIQIGssXFlE2RNAHrO08dct0cFpe41uF5Y8WWh4DiNitpydJfOk9G/Itfm/53
g9Ci5UKFB4+YvGrqMz+StypOWO3syrEzYJf2Sv/Xh1wInPDUboQ8gFev9Gzc3LG5
8pcflcVN21GGYuxH3f4KdR5LmgFdYWcPDvY76B9tNWw0bPHUzU8=
=7Aiz
-----END PGP SIGNATURE-----
```

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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 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

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