secuvera-SA-2021-01: Privilege Escalation in NetSetMan Pro 4.7.2

From: Simon Bieber <sbieber () secuvera de>
Date: Fri, 11 Jun 2021 09:54:44 +0200

```
-----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-----

iQIzBAEBCAAdFiEE6mgEBCu3JYBqmGrgDIJc8mYSY6UFAmDDFocACgkQDIJc8mYS
Y6V1YBAAivvBI79oAYKrkkELU1drnEtIloRggLF6FQ4BlBgZ1DMfLQLcbACVT2LY
ro9SBpU/s6AOaZ98jETA/nS57MD+70ncEevP6hm3DzxV1mHtS4rjTU6hkcFfC8tq
rqeXRz4t1oWhPQd+AB2TOvpUIRtVn4zomNs9e3YkYRhRBixqZgrLz/c0mQjKIW/u
+hf0v5RYYSwA8q9LyhN6QUmm0UCVg06o55l8+eyc6V1JeMekdX7ais99Ki/FNmYw
z66aP4FrPx+RpCVsl0sCpMiZWIhNtUVq37uNJCaE55K6li241RVDLmzZtNFThx8F
maqdUa1wdEJ3AY8Ays/s2HWg4EkTyA1Key25NvSUVNUvYwqDgE/TzXK/rqVpIvIs
+dTiEJ1Q8aBlRL61UF6ddz2fliVj85q/4tQCJ/Nk062pkpI2bfhsgeEnwwkXQrTp
Yqln1z0R4THpWsiUQ0q3VeFFDU33T8Lch1wpURNtR1V1O+Zz4T4W+UX5Q3uIfprF
04TwIQIGssXFlE2RNAHrO08dct0cFpe4luF5Y8WWh4DiNitpydJfOk9G/Itfm/53
g9Ci5UKFB4+YvGrqMz+StypOWO3syrEzYJf2Sv/Xh1wInPDUboQ8gFev9Gzc3LG5
8pcflcVN2lGGYuxH3f4KdR5LmgFdYWcPDvY76B9tNWw0bPHUzU8=
=7Aiz
-----END PGP SIGNATURE-----
```

Current thread:

- **secuvera-SA-2021-01: Privilege Escalation in NetSetMan Pro 4.7.2** ***Simon Bieber (Jun 11)***

Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License