

NT-Bugtraq: [NGSEC-2004-7] NtRegmon, local system denial of service.

[NGSEC-2004-7] NtRegmon, local system denial of service.

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-08/0114.html>

From: NGSEC (labs_at_NGSEC.COM)

Date: 08/25/04

Date: Wed, 25 Aug 2004 11:34:37 +0200
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Next Generation Security Technologies
<http://www.ngsec.com>
Security Advisory

Title: NtRegmon, local system denial of service.

ID: NGSEC-2004-7

Application: NtRegmon (<http://www.sysinternals.com/ntw2k/source/regmon.shtml>)

Date: 14/Aug/2004

Status: Patched version available (6.12).

Platform(s): Windows OSs.

Author: Fermín J. Serna <fjserna@ngsec.com>

Location: <http://www.ngsec.com/docs/advisories/NGSEC-2004-7.txt>

Overview:

NtRegmon is a Registry monitoring utility that will show you which applications are accessing your Registry, which keys they are accessing, and the Registry data that they are reading and writing – all in real-time.

For its task NtRegmon hooks some kernel mode functions (Registry functions) for its logging purposes.

Regmon suffer from an unvalidated pointer referencing in some of this kernel hooks.

While any privileged user is using NtRegmon, any local and unauthorized user can crash the system.

Technical description:

NT-Bugtraq: [NGSEC-2004-7] NtRegmon, local system denial of service.

NtRegmon is a Registry monitoring utility that will show you which applications are accessing your Registry, which keys they are accessing, and the Registry data that they are reading and writing – all in real-time.

For its task NtRegmon hooks some kernel mode functions (Registry functions) for its logging purposes.

Regmon suffers from some unvalidated pointer referencing in some of its kernel hooks. In example NtRegmon hooks ZwSetQueryValue declared as follows:

```
NTSTATUS ZwSetQueryValue(DWORD KeyHandle, DWORD ValueName, DWORD TitleIndex,
                        DWORD Type, DWORD Data, DWORD DataSize);
```

The problem exists because NtRegmon does not properly check if some argument pointers are valid or not. While any privileged user is using Regmon, any local and unauthorized user can crash the system.

Sample exploitation can be found:

<http://www.ngsec.com/downloads/exploits/ntregmon-dos.c>

Recommendations:

Upgrade to NtRegmon version 6.12.

More security advisories at: <http://www.ngsec.com/ngresearch/ngadvisories/>

PGP Key: <http://www.ngsec.com/pgp/labs.asc>

Copyright(c) 2002-2004 NGSEC. All rights reserved.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.4 (GNU/Linux)

iD8DBQFBLFeCKrwoKcQI8Y4RAjxYAKCYw9QhDRCxnJSXd2HFt9Zp/pRgYwCfQynV

/bd12s6PNLcuP6kXn5pRS1g=

=P5Yq

-----END PGP SIGNATURE-----

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.
