Posted by *Parvez* on *November 13, 2017*

IKARUS anti.virus and its 9 exploitable kernel vulnerabilities

Posted in: All, Bugs, Exploits, Vulnerabilities. Tagged: Elevate, Kernel. 5 comments

Here is a list of the 9 kernel vulnerabilities I discovered over a month ago in an antivirus product called IKARUS anti.virus which has finally been fixed. Most of the vulnerabilities were due to the inputted output buffer address (Irp->UserBuffer) being saved on the stack which is later used without being validated when using as an argument. The table below lists the ioctls, related CVE and type of vulnerability

IOCTL	CVE ID	Vulnerability Type
0x8300000c	CVE-2017-14961	Arbitrary Write
0x83000058	CVE-2017-14962	Out of Bounds Write
0x83000058	CVE-2017-14963	Arbitrary Write
0x8300005c	CVE-2017-14964	Arbitrary Write

Recent Posts

- Exploiting System Shield AntiVirus Arbitrary Write Vulnerability using SeTakeOwnershipPrivilege
- IKARUS anti.virus and its 9 exploitable kernel vulnerabilities
- Exploiting Vir.IT eXplorer Anti-Virus Arbitrary Write Vulnerability
- Running Macros via ActiveX Controls
- Spraying the heap in seconds using ActiveX controls in Microsoft Office

Categories

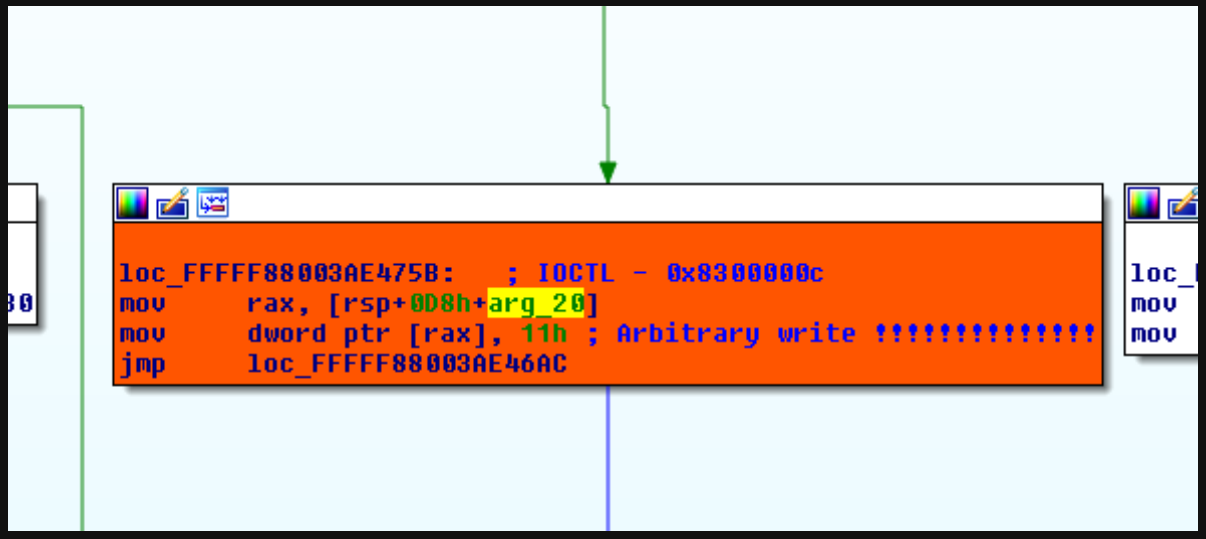
- All
- Bugs
- Exploits
- Malware
- Mitigation

0x830000cc	CVE-2017-14965	Arbitrary Write
0x830000c0	CVE-2017-14966	Arbitrary Write
0x83000080	CVE-2017-14967	Arbitrary Write
0x830000c4	CVE-2017-14968	Arbitrary Write
0x83000084	CVE-2017-14969	Arbitrary Write

Fixed version numbers (vendors advisory ~~soon to be released~~)

	Vulnerable version	Fixed version
Software	2.16.7	2.16.18
ntguard.sys	0.18780.0.0	0.43.0.0
ntguard_x64.sys	0.18780.0.0	0.43.0.0

I'm exploiting the vulnerable subroutine used by ioctl 0x8300000c by overwriting the _SEP_TOKEN_PRIVILEGES structure where arg_20 is our inputted output buffer address.



- Other
- Vulnerabilities

Tags

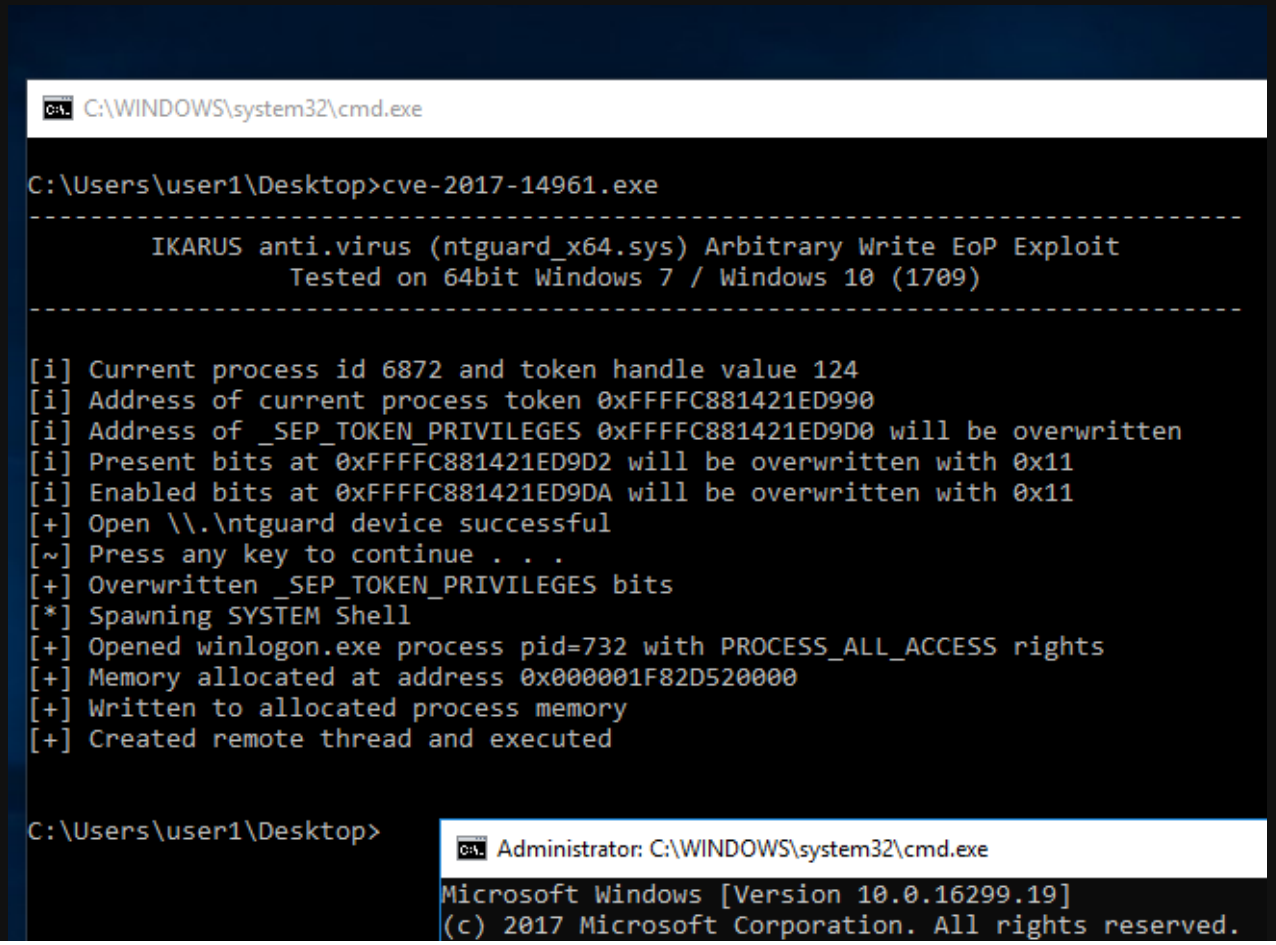
ActionScript ActiveX Adobe Anti-Rootkit ASLR Autorun BHO BlazeDVD Download and Execute Elevate EMET FakeAV heapspray Hidden Hijack IrfanView Java Kernel Macros McAfee MSI MSWord PGP pif RemoteExec Return to Libc ROP Sandbox Skype SureThing Symantec trailing UAC URI Vista

Archives

- January 2018 (1)
- November 2017 (2)
- September 2016 (1)
- December 2015 (2)
- July 2015 (1)
- January 2015 (1)
- December 2014 (1)
- June 2014 (1)
- January 2014 (1)
- November 2013 (1)
- September 2013 (1)
- February 2013 (1)
- December 2012 (1)
- August 2012 (1)

In our process _SEP_TOKEN_PRIVILEGES structure I'm overwriting a byte in the "Present" field and a byte in the "Enabled" field with the hardcoded value of 0x11 by calling the vulnerable subroutine twice.

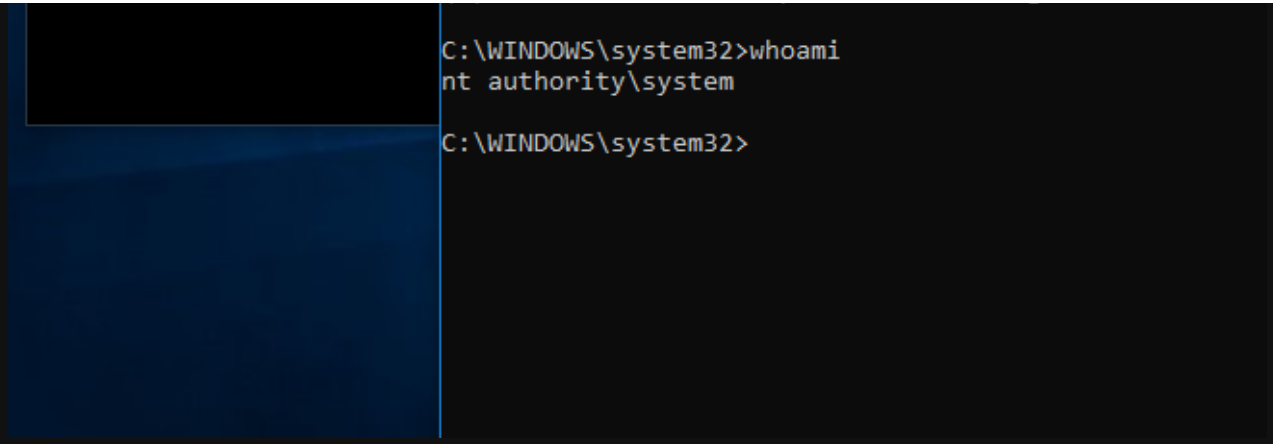
```
DeviceIoControl(hDevice, 0x8300000c, NULL, 0,
(LPVOID)PresentByteOffset, 0, &dwRetBytes, NULL);
DeviceIoControl(hDevice, 0x8300000c, NULL, 0, (LPVOID)EnableByteOffset,
0, &dwRetBytes, NULL);
```



- June 2012 (1)
- February 2012 (1)
- January 2012 (1)
- December 2011 (1)
- November 2011 (1)
- August 2011 (2)
- July 2011 (1)
- April 2011 (1)
- March 2011 (1)
- October 2010 (3)
- June 2010 (1)
- May 2010 (1)
- March 2010 (2)
- February 2010 (1)
- December 2009 (1)
- September 2009 (1)
- May 2009 (1)
- April 2009 (1)
- September 2008 (1)
- November 2007 (2)

Meta

- Log in
- Entries RSS
- Comments RSS
- WordPress.org



The exploit can be downloaded from here [zip] or from Exploit-DB when it gets published.

@ParvezGHH

← Exploiting Vir.IT eXplorer Anti-Virus Arbitrary Write Vulnerability

Exploiting System Shield AntiVirus Arbitrary Write Vulnerability using SeTakeOwnershipPrivilege →

5 comments on “IKARUS anti.virus and its 9 exploitable kernel vulnerabilities”

Alex

on February 15, 2018 at 2:50 pm said:

You can upload the ntguard_x64.sys & ntguard.sys [0.18780.0.0]

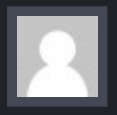
I checked their site and they do not have old versions.

Kind regards,

Parvez

on February 15, 2018 at 3:18 pm said:

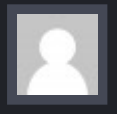
Here are the vulnerable drivers of Ikarus Antivirus https://www.greyhathacker.net/docs/ntguard.zip



Alex

on February 15, 2018 at 4:36 pm said:

Many thanks!
it's working with winlogon.exe but doesn't work with csrss.exe. =c



Alex

on February 15, 2018 at 4:37 pm said:

win 10 x64 (Unable to open csrss.exe process)

Parvez

on February 15, 2018 at 5:39 pm said:

You should be able to open the process (unless there are other restrictions) but I noticed CreateRemoteThread api doesn't work so you might need to research into another method to

execute the code.

Leave a Reply

Your email address will not be published. Required fields are marked *

* Name

* Email

Website

Save my name, email, and website in this browser for the next time I comment.

I'm not a robot

reCAPTCHA
Privacy - Terms

Post Comment

Proudly powered by WordPress Theme: Parament by Automattic.