IOActive Security Advisory

Title	TVSUkernel Escalation of Privileges
Severity	Critical
Discovered by	Sofiane Talmat
Advisory Date	November 19, 2015
CVE	CVE-2015-8110

Affected Products

Lenovo System Update (Discovered in version 5.07.0013)

Impact

This vulnerability allows a local unprivileged user to run commands as the Windows SYSTEM user.

Background

The Lenovo System Update allows least-privileged users to perform system updates. To do this, System Update includes the System Update service (SUService.exe). This service runs as the privileged SYSTEM user, creates a temporary user account with Administrator privileges, and starts a GUI application (Tvsukernel.exe) with the new Administrator account. Once the application is closed, the temporary Administrator account is appropriately deleted. However the GUI application contains links to online support and privacy help topics, which, when clicked, start a web browser instance under the temporary Administrator account to display the online topic.

As a result, an attacker who is unprivileged can exploit the web browser instance that is running as Administrator to elevate his or her own privileges to Administrator or SYSTEM.

Technical Details

IOActive executed the following steps to create a Proof of Concept:

1- Start the Lenovo System Update application.



- 2- Click one of two following links to allow the execution of a web browser with Administrator privileges:
 - a. "Click here to learn more" link on the main window

Restore hidden updates	for restoring the hidden updates. Click Next to Get new updates.					
	Note: Some of the update operating system is most Click here to learn more.	st up-to-date by runni		ts. Ensure that	your Windows	
D PCDSchema2_	_31.xsd	3/27/2014 4:15 PM	XML Schema File	38 KB	Next >	
SocksSSLConr						
StartServiceLo	gger.txt	10/30/2015 4:10 AM	Text Document	1 KB		

b. The Help icon 🗳 at top right > Settings > View Privacy Policy link

System Update ^{ick} (C) → 1	Program Files (x86) → Lenovo → System Update → · · · · · · · · · · · · · · · · · ·
Welcome	Welcome to System Update.
Get new updates	You can use this tool to search for new updates for your computer, review them, then select the ones you want to download and install.
Install deferred updates	Select Schedule updates in the left pane to download and install updates automatically or receive notifications when updates
Advanced	View installation biotom shows the status version and dates of the underse were installed and the status of the underse were installed and th
Schedule updates	You This application lets you share optional usage statistics with Lenovo to help time. Select us improve our software.
View installation history	In ac View privacy policy s; yet have len updates for re
Restore hidden updates	Click Next to Get new updates.
	Note. Sense of the updates depende en certain Windows Comparents. Encore that your Windows operating system is most up-to-date by running Windows Updates. Click here to learn more.
DPCDSchema2	31.xsd 3/27/2014 4:15 PM XML Schema File 38 KB
SocksSSLConr	nector.dll 9/29/2015 11:14 AM Application extens 66 KB



y using this website you allow us to place cookies on your computer. They are harmless and never personally identify you. Conti SHOP DEALS SUPPORT Official Lenovo Support Home Documents File Options View Help Applications Processes Services Performance Networking Users Image Name CPU Memory (UAC Virtual Description cress.exe v-sotalm 00 1,556 K Deabled Desktop updates for your computer image Name Option (UAC Virtual Description symptom v-sotalm 00 4,348 K Deabled Microsoft Symptom Vour computer is installed with the ThinkVantage System on certain Windows components. If you do not run Window without some Windows updates such as updates for Hother 0 4,360 K Disabled Windows Processe: 57 CPU Usage 0% Physical Memory : 33% Citck here to citck									
SHOP DEALS SUPPORT Official Leavov Support Home Documents File Options View Help Applications Processes Services Performance Networking Users Image Name User Name OP Memory (UAC Virtual Description inage Name User Name OP Memory (UAC Virtual Description inage Name User Name OP Memory (UAC Virtual Description inage Name User Name OP 1,580 K Usabled Description inage Name User Name OP 1,580 K Usabled Windows inage Name User Name OP 4,540 K Usabled Windows inage Name User Name OP 4,540 K Usabled Microsoft inage Name Visotan OP 4,540 K Disabled Microsoft inaddros zero Visotan OP 3,200 K Disabled Windows isotan OP 1,297 K Disabled Windows isotan	🕞 🕘 🦉 https://support.lenovo.com/us/er 🔎 < 🖉 Run Windows Update befo 🗴								
SHOP DEALS SUPPORT Official Lenovo Support Houe Documents File Options View Help Applications Processes Services Performance Networking Users Num Windows Updates O 1,56 K Disabled Desktop Excitors updates for your computer Symptom 0 32,208 K Disabled Microsoft Internet Internet<	By using this website you allow us to place cookies on you	r computer. They are ha	rmless and never perso	nally i	dentify you.			Continu	
Official Lenovo Support Home Documents Applications Yiew Help Applications Processes Services Performance Networking Users Image Name User Name OU 1,580 K Deabled Desktop Image Name updates for your computer installed with the ThinkVantage System on certain Windows components. If you do not run Window without some Windows updates such as updates for Horitor. Visual mode with some Visual mode without some Windows updates such as updates for Horitor. Affected configurations Forcesses: 17 CPU Usage: 0% Physical Memory: 33% Click here to retain some	j Windows Task Manager								
Official Lenovo Support Home Documents Image Name User Name CPU Memory (UAC Virtuali Description Symptom 00 1,556 X Disabled Desktop Symptom 00 4,374 K Internet Vour computer is installed with the ThinkVantage System on certain Windows updates such as updates for try windows and true Windows 00 1,256 K Disabled Microsoft VOur computer is installed with the ThinkVantage System ONENOTEM.EXE *32 v-sotalm 00 1,256 K Disabled Windows VINCServer.exe ***** v-sotalm 00 4,360 K Disabled Hortrow fill Microsoft ONENOTEM.EXE *32 v-sotalm 00 12,976 K Disabled Microsoft UNCServer.exe ************************************	SHOP DEALS SUPPORT	File Options View H	lelp						
Image Name User Name CPU Memory (UAC Virtual Description Run Windows Update buddetes for your computer 00 1,580 K 00 25,272 K Disabled Desktop Windows To your computer 00 1,156 K Disabled Mindows Internet Explore.exe v-sotalm 00 43,784 K Internet Image Name V-sotalm 00 43,784 K Internet Non-cave *32 V-sotalm 00 43,784 K Internet Non-cave *32 V-sotalm 00 43,784 K Internet Symptom Vour computer is installed with the ThinkVantage System on certain Windows components. If you do not run Window without some Windows updates such as updates for Hothr 00 2,528 K Disabled Windows Affected configu	the second of th	Applications Processes	Services Performance I	Vetwork	king Users				
Run Windows Updateb updates for your comput Crrs.exe v-sotalm 00 1,580 K Disabled Desktop Symptom Southication.exe *32 v-sotalm 00 32,208 K Disabled Microsoft Symptom 00 12,976 K Disabled Microsoft ONES.EXE *32 v-sotalm 00 4,848 K Disabled Microsoft Symptom Vour computer is installed with the ThinkVantage System on certain Windows components. If you do not run Window without some Windows updates such as updates for Hotfax V-sotalm 00 2,528 K Disabled Windows Affected configurations Processes: 57 CPU Usage: 0% Physical Memory: 33% Click here to rate this page	Official Lenovo Support Home Documents								
Run Windows Update by updates for your computer is installed with the ThinkVantage System on certain Windows updates such as updates for Hotikr 0 2,522 k Disabled Microsoft Unit windows Unit windows Unit windows Unit windows updates such as updates for Hotikr Affected configurations Affected configurations C UPU Usage: 0% Physical Memory: 33%		Image Name	User Name	CPU	Memory (UAC Virtuali	Description		
Run Windows Update buddets for your computer explore.exe v.sotalm 00 26,272 k Disabled Windows Bymptom windows components. If you do not run Window wurdates such as updates for Hotfking 00 43,784 k Internet Internet Affected configurations Mindows updates such as updates for Hotfking Viscal Memory: 33% O 43,784 k Internet Click here to rate this part of the p		csrss.exe		00	1,580 K				
Run Windows Update buddets updates for your computer Image: space and		dwm.exe	v-sotalm	00	1,156 K	Disabled	Desktop		
updates for your comput iexplore.exe *32 t/su_mp_eqmqeNLIWS 00 43,784 k Internet updates for your comput worker 00 32,208 k Disabled Microsoft Symptom 00 804 k Disabled Schothic Schothic Your computer is installed with the ThinkVantage System on certain Windows components. If you do not run Windwith without some Windows updates such as updates for Hotfix Viscure * *32 v-sotalm 00 12,976 k Disabled Wircosoft Affected configurations Windows updates such as updates for Hotfix UNCServer exe *32 v-sotalm 00 5,624 k Disabled Wirdows Processes from all users End Process 00 2,064 k VirtualBox End Process Click here to rate this processes from all users Click here to rate this process	Deve Winderer II. 1-4-1	explorer.exe	v-sotalm	00	26,272 K	Disabled	Windows		
updates for your comput iexplore.exe *32 t/su_mp_eqmqeNLIWS 00 43,784 k Internet updates for your comput worker 00 32,208 k Disabled Microsoft Symptom 00 804 k Disabled Schothic Schothic Your computer is installed with the ThinkVantage System on certain Windows components. If you do not run Windwith without some Windows updates such as updates for Hotfix Viscure * *32 v-sotalm 00 12,976 k Disabled Wircosoft Affected configurations Windows updates such as updates for Hotfix UNCServer exe *32 v-sotalm 00 5,624 k Disabled Wirdows Processes from all users End Process 00 2,064 k VirtualBox End Process Click here to rate this processes from all users Click here to rate this process	Kun windows Update b	G	tvsu_tmp_eqmqeNLIWS	00	6,140 K		Internet		
Symptom MSECSCR. * v - sotalm 00 NO 44 Disabled Send to O Symptom SCNotification.exe *32 v-sotalm 00 4,360 K Disabled Send to O Your computer is installed with the Think/Vantage System on certain Windows components. If you do not run Window without some Windows updates such as updates for Hotfix UNCServer.exe *32 v-sotalm 00 5,624 K Disabled UNCServer Affected configurations Windows updates such as updates for Hotfix Processes from all users End Process End Process Click here to rate this page Click here to rate this page. Click here to rate this page.		iexplore.exe *32	tvsu_tmp_eqmqeNLIWS	00	43,784 K		Internet		
Symptom MSECSCR. * v - sotalm 00 NO 44 Disabled Send to O Symptom SCNotification.exe *32 v-sotalm 00 4,360 K Disabled Send to O Your computer is installed with the Think/Vantage System on certain Windows components. If you do not run Window without some Windows updates such as updates for Hotfix UNCServer.exe *32 v-sotalm 00 5,624 K Disabled UNCServer Affected configurations Windows updates such as updates for Hotfix Processes from all users End Process End Process Click here to rate this page Click here to rate this page. Click here to rate this page.	updates for your compu	lync.exe *32							
Symptom Symptom Solutification.exe *32 v-sotalm Solutification	1 7 1								
Symptom Symptom Your computer is installed with the ThinkVantage System on certain Windows components. If you do not run Windo without some Windows updates such as updates for Hotfxi Affected configurations									
Symptom Your computer is installed with the ThinkVantage System on certain Windows components. If you do not run Window without some Windows updates such as updates for Hotfxi									
Your computer is installed with the Think Vantage System on certain Windows components. If you do not run Window without some Windows updates such as updates for Hoffix Visukernel.exe *32 visutimp_eqmqeNLTWS 00 17,604 K Lenovo S Affected configurations Windows Visutimp_eqmqeNLTWS 00 1,356 K Disabled VINCServer Processes: 57 CPU Usage: 0% Physical Memory: 33% End Process	Symptom		· Socialiti						
Your computer is installed with the ThinkVantage System on certain Windows components. If you do not run Windd without some Windows updates such as updates for Hotfix UNCServer.exe *32 v-sotalm 00 5,624 K Disabled UNCServer Affected configurations UNCServer.exe *32 v-sotalm 00 2,064 K UNCServer VirtualBox Processes: 57 CPU Usage: 0% Physical Memory: 33% Click here to rate this page	oympioni					Disabled			
Your computer is installed with the ThinkVantage System on certain Windows components. If you do not run Window without some Windows updates such as updates for Hotfix VBoxTray.exe windogon.exe v-sotalm 00 1,356 K Disabled VirtualBox Affected configurations VBoxTray.exe v-sotalm 00 1,356 K Disabled VirtualBox Processes: 57 CPU Usage: 0% Physical Memory: 33% Click here to rate this page						Disphlad			
on certain Windows components. If you do not run Window without some Windows updates such as updates for Hotfix Affected configurations Processes: 57 CPU Usage: 0% Physical Memory: 33% Click here to rate this page	Your computer is installed with the Think Vantage Sustem								
without some Windows updates such as updates for Hotfix Affected configurations Processes: 57 CPU Usage: 0% Physical Memory: 33% Click here to rate this page			v-soldini			Disableu	vii tudibux		
Affected configurations Processes: 57 CPU Usage: 0% Physical Memory: 33% Click here to rate this page		- millogonicke			2,00110				
Click here to rate this page	winout some windows appares such as appares for from	Show processes fro	om all users					End Process	
Click here to rate this page	Affected configurations	Dragosson 57 CDUU	leage 0% Dhusi	cal Ma	mon # 22%				
rate this page	Anteres comparators	Processes: 57 CPU (Physi		mory: 35%				
rate this page	-							Click here to	
	The above symptom is associated with, but not limited to, the	following systems:						rate this page	

3- Next, an instance of the web browser will run as Administrator.

4- Elevate the attacker's privileges to Administrator and SYSTEM through the web navigator instance that is running as Administrator.

Fixes

Install the latest version of the Lenovo System Update application (version 5.06.0043 or higher), which is available through System Update.

Lenovo also has issued an advisory about this vulnerability: https://support.lenovo.com/us/en/product_security/lsu_privilege.

Timeline

October 2015 – IOActive discovers the privilege escalation vulnerability

November 2, 2015 – IOActive reports it to Lenovo

November 19, 2015 – Lenovo releases a fix and advisory