

## 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.

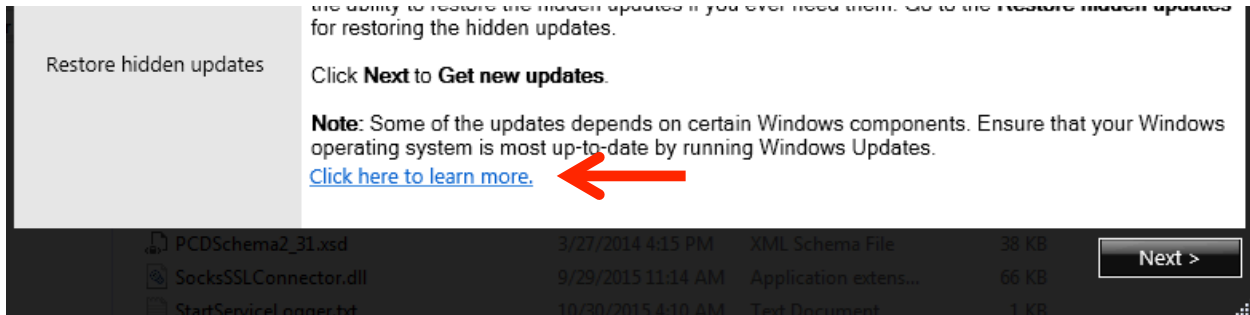
### Technical Details


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

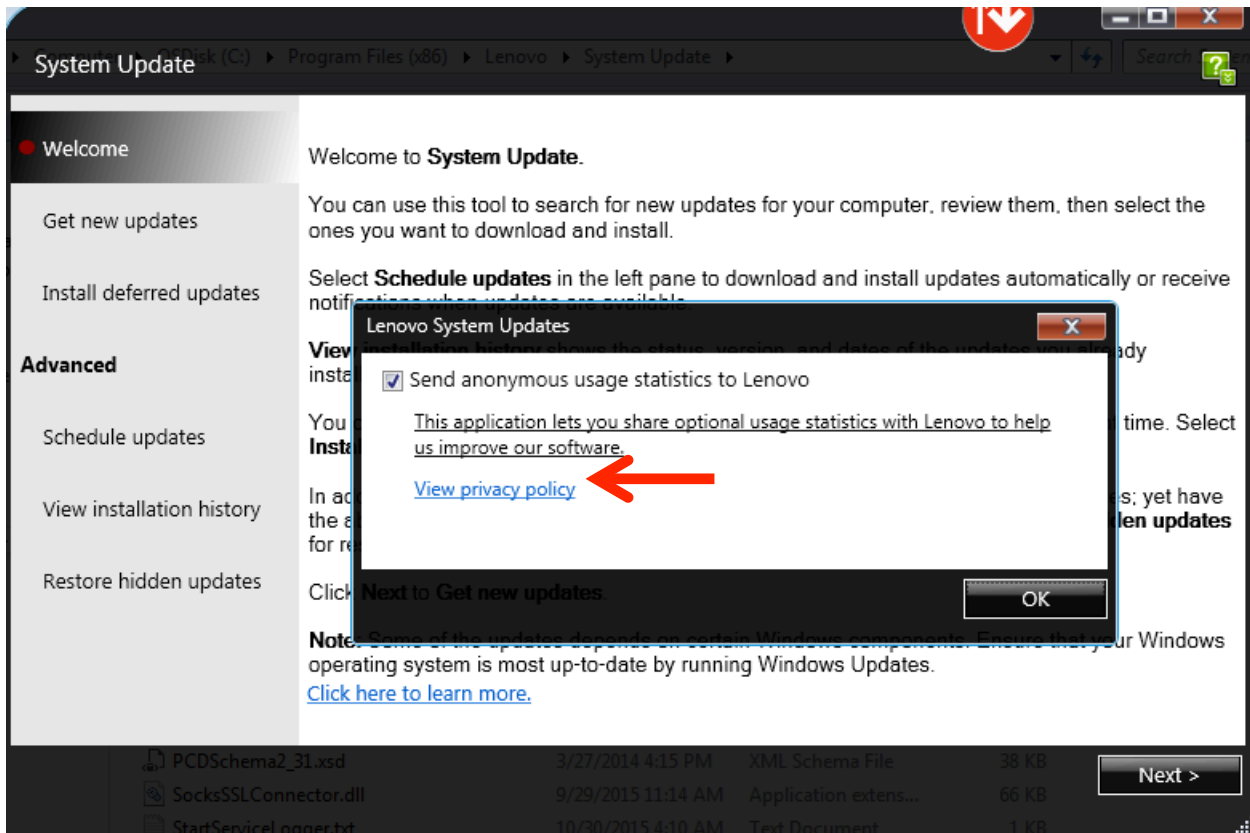
- 1- Start the Lenovo System Update application.

2- Click one of two following links to allow the execution of a web browser with Administrator privileges:

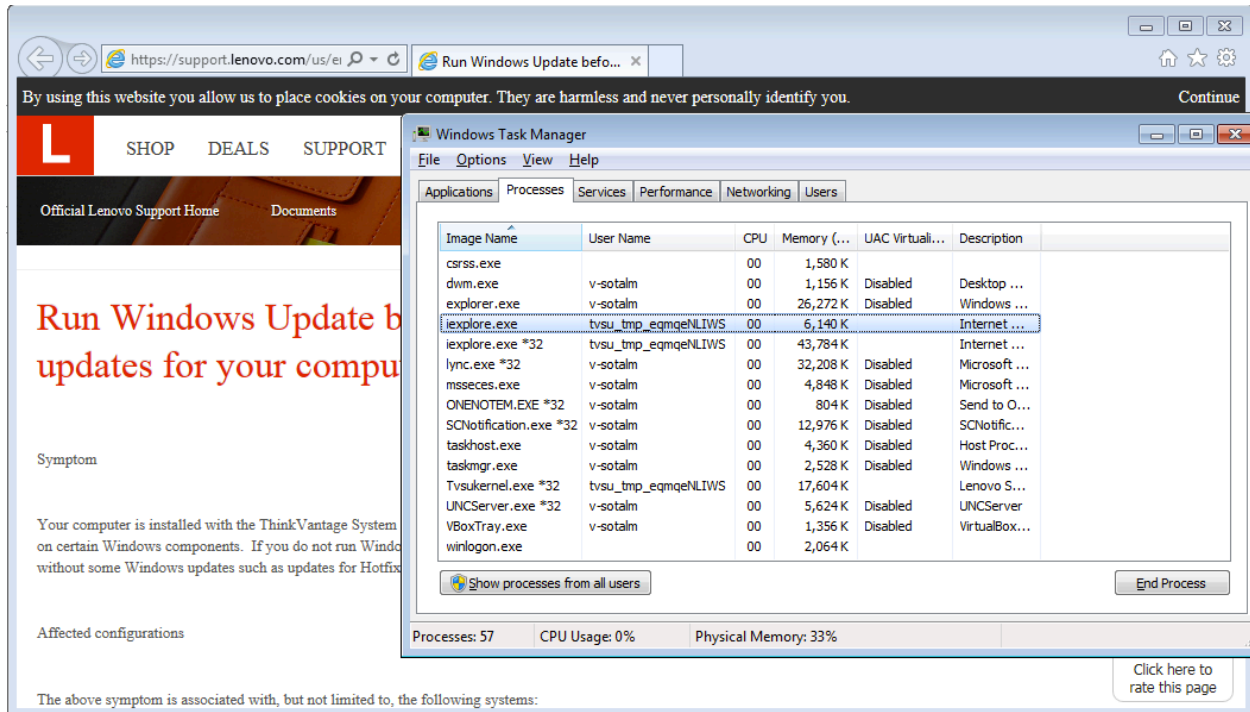
a. “Click here to learn more” link on the main window



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



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](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