IOActive Security Advisory

Title	System Update Created an Insecure Random Administrator Password
Severity	Critical
Discovered by	Sofiane Talmat
Advisory Date	November 19, 2015
CVE	CVE-2015-8109

Affected Products

Lenovo System Update (Discovered in version 5.07.0013)

Impact

This vulnerability allows an attacker to acquire Administrator privileges on a machine by predicting the username and password of the temporary Administrator account.

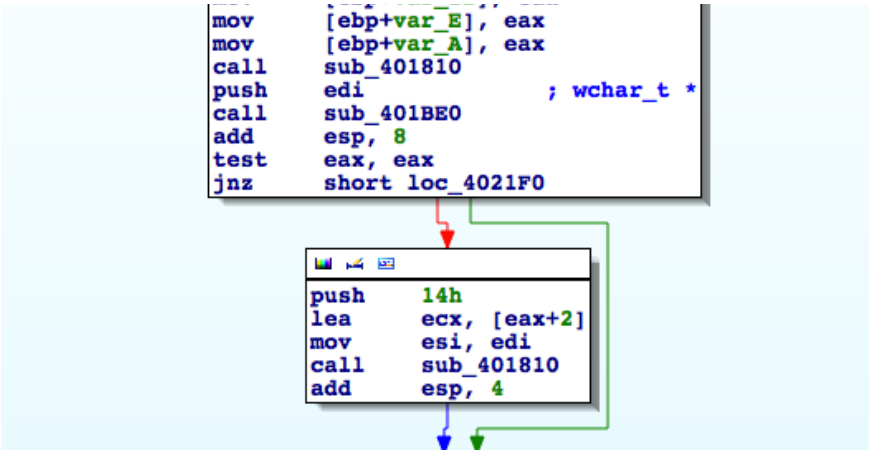
Background

This vulnerability allows a local unprivileged user to elevate privileges to Administrator or SYSTEM. Since the user is running the System Update is an unprivileged user, the SUService that is running as System will run the UACsdk.exe binary to create a temporary Administrator account to run the GUI application (Tvsukernel.exe).

Lenovo creates a random temporary Administrator account with a username that follows the template tvsu_tmp_xxxxxXXXXX, where each lowercase x is a randomly generated lower case letter and each uppercase X is a randomly generated uppercase letter. A 19-byte, random password is generated via an algorithm.

Technical Details

The execution flow is as follows:



The function sub_401810 accepts three arguments and is responsible for generating a random alphanumeric username value with the third argument length.

The first call to this function generates 10 alphanumeric bytes as a suffix for the Administrator username, following the template form tvsu_tmp_xxxxxXXXXX.

The function sub_401810 uses a predictable algorithm to generate the random alphanumeric sequence based on a sequence of calls to the rand function after setting a seed using the srand relaying on _time64 and an initial call to rand.

Due to this weakness, an attacker who knows the account creation time can predict the generated username using the same algorithm.

Lenovo uses stronger random pattern generation (Method #1) for the password through the function sub_401BE0 with Microsoft Crypto API CryptGenRandom. If Method #1 fails to acquire Crypto Context (CryptAcquireContextW) or fails to generate either the random value or the hash, the execution fails back to a call to sub_401810 and uses the previous predictable rand-based algorithm to generate the password. In other words, an attacker could predict the password created by Method #2.

In summary, an attacker could under certain circumstances predict both the username and password of the temporary Administrator account and use this access to acquire Administrator privileges on the machine.

Solution

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.

History

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

