

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE ISSUED:

08/14/2015

SUBJECT:

Vulnerability in Lenovo Service Engine (LSE) Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Lenovo Service Engine utility which could allow for remote code execution. Lenovo Service Engine is a utility found in the BIOS that installs and updates Lenovo software. Successful exploitation of this vulnerability may allow an attacker to gain control of the utility and perform unauthorized actions.

THREAT INTELLIGENCE:

Proof of concept code does exist. There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

Lenovo Desktop Models Running Windows 8 or 8.1:

A540/A740

B4030

B5030

B5035

B750

C2005

C4005

C2030/C4030

C260

C5030

H3000

H3050

H5000

H5055

H5050

Horizon2 27

Horizon 2e(Yoga Home 500)

Horizon 2S

X310(A78)

X315(B85)

Lenovo Laptop Models Running Windows 7,8, 8.1 and 10:

Flex 2 Pro-15/Edge 15 (Broadwell)

Flex 2 Pro-15/Edge 15 (Haswell)

Flex 3-1470/1570
Flex 3-1120
G40-80/G50-80/G50-80 Touch/V3000
S21e
S41-70/U41-70
S435/M40-35
Yoga3 14
Z70-80 / G70-80
Yoga 3 11
Y40-80
Z41-70/Z51-70

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

A vulnerability has been discovered in Lenovo Service Engine utility which could allow for remote code execution. The vulnerability can be exploited by an attacker performing a buffer overflow attack. Successful exploitation could result in an attacker gaining access to the utility and installing malicious software that will always run upon boot-up of the machine even after it has been re-imaged.

Please note that the vulnerability only applies to Lenovo laptop computers running Windows 7, 8, 8.1 and 10.

Additionally, this vulnerability only applies to Lenovo desktop computers that were manufactured between 10/23/14 and 4/10/15, running Windows 8 and 8.1.

RECOMMENDATIONS:

The following actions should be taken:

Download and run the disabler tool provided by Lenovo.

Remind users not to download, accept, or execute files from un-trusted or unknown sources.

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Lenovo:

https://support.lenovo.com/us/en/product_security/lse_bios_notebook

https://support.lenovo.com/us/en/product_security/lse_bios_desktop

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

