



## UNCLASSIFIED

*This Cyber Note is a joint product produced by the Oklahoma Cyber Command/Security Operations Center and the Oklahoma Information Fusion Center.*

### **CYBER NOTE: Vulnerable Adware pre-loaded on Lenovo PCs**

**INFORMATION:** This is a critical cybersecurity alert concerning the possibility of adware being preloaded on Lenovo PCs.

The adware application, called Visual Discovery, made by an Israeli company called Superfish was loaded and distributed on Lenovo PCs sold between October and December 2014; potentially as early as 2010.

Visual Discovery is reported to install as a self-signed root certificate that intercepts encrypted web traffic for websites a user visits. This "hijacking" of the SSL could allow for malicious websites to masquerade as legitimate trusted sites. This allows the application to hijack the user's SSL session to a secured website, decrypt the secure session and then re-encrypt the session again. Because the certificates used by Superfish are signed by the certification authority (CA) installed by the software, the browser will not display any warnings that the traffic is being tampered with. The same cryptographic key is reportedly used on all the installations on Lenovo systems containing the software made by Superfish.

It is also reported that the local private key for the Superfish CA certificate has been cracked and now is readily available for use in the wild. This could allow for man-in-the-middle style attacks against these systems.

Lenovo has released a list of models that may have had Visual Discovery by Superfish installed sold between October and December 2014:

- G Series: G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45
- U Series: U330P, U430P, U330Touch, U430Touch, U530Touch
- Y Series: Y430P, Y40-70, Y50-70
- Z Series: Z40-75, Z50-75, Z40-70, Z50-70
- S Series: S310, S410, S40-70, S415, S415Touch, S20-30, S20-30Touch
- Flex Series: Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 14(BTM), Flex2 15(BTM), Flex 10
- MIIX Series: MIIX2-8, MIIX2-10, MIIX2-11
- YOGA Series: YOGA2Pro-13, YOGA2-13, YOGA2-11BTM, YOGA2-11HSW
- E Series: E10-30]

Lenovo states they have discontinued the practice of pre-installing Superfish Visual Discovery; however, the systems that came with the software already installed will continue to be vulnerable until actions have been taken.

**RECOMMENDATIONS:** The following actions are suggested by the Oklahoma Cyber Command Security Operations Center to re-mediate the potential vulnerability:

- Wipe the system and install a non-Lenovo shipped operating system, such as your organization's enterprise licensed copy of an operating system.

If the above option is not available, the following recommendations are suggested:

- Manually remove the Superfish root certificate. One method to accomplish this is to do the following (administrator level access is required):
  - Click the Windows icon at the bottom left corner of the screen.
  - Type "cmd.exe" into the resulting search field and hit the enter key.
  - Type "certmgr.msc" at the command-prompt in the resulting terminal window and hit enter.
  - Select "Trusted Root Certification Authorities" in the left-hand navigation window of the resulting dialogue box, then select "Certificates."
  - Select Superfish and/or Visual Discovery. Right-click and select "Delete."
  - You may have to reboot the PC to effect the change

**OKLAHOMA IMPACT:** This information is being shared for your situational awareness and computer/network defenses. Contact your trusted IT services organization for further information.

**FEEDBACK:** Please take a moment to complete this brief survey and help evaluate the quality, value, and relevance of our products. Your response will help us serve you more effectively and efficiently in the future. Thank you for your assistance. Click the link below to take the survey. If the link does not work, copy and paste it into your browser.

[https://www.surveymonkey.com/s/Oklahoma\\_Information\\_Fusion\\_Center](https://www.surveymonkey.com/s/Oklahoma_Information_Fusion_Center)

**SOURCES:**

Oklahoma Management and Enterprise Services – Oklahoma Cyber Command  
US-CERT <https://www.us-cert.gov/ncas/alerts/TA15-051A>

**TRACKING NUMBER:** CN 2015-120934; HSEC 1.8, 1.10

**WARNING:** This document is **UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO)** and is for official use only. Wide release of this information could adversely affect or jeopardize investigative activities. It contains information that may be exempt from public release under the Oklahoma Open Records Act (51 O.S. 24A.8). It is not to be released to the public, the media, or other personnel who do not have a valid need-to-know without prior approval of the OIFC. State and Local law enforcement officials may share this information with authorized critical infrastructure and key resources personnel and other necessary private sector security officials without further approval from OIFC.

**Oklahoma Information Fusion Center**

**Watch Desk**

**405.842.8534 phone**

**405.879.2967 fax**

[fusion@osbi.ok.gov](mailto:fusion@osbi.ok.gov)

The information contained in this document is the property of the Oklahoma Information Fusion Center (OIFC) and may be exempt from public release under the Freedom of Information Act (5 USC 552). This document is to be controlled, handled, transmitted, and distributed in accordance with classification markings contained within. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access.