National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Advisory

Komodia Redirector with SSL Digestor fails to properly validate SSL and installs non-unique root CA certificates and private keys (Superfish Vulnerability)

Original Issue Date: 25th February 2015

Severity Rating: High

Potential Security Impact: Man-in-the-Middle Attack

Software Affected:

- Lenovo Notebooks Models:
  - E-Series: E10-30
  - Flex-Series: Flex2 14, Flex2 15, Flex2 14D, Flex2 15D, Flex2 Pro, Flex 10
  - G-Series: G410, G510, G710, G40-30, G40-45, G40-70, G40-80, G50-50, G50-45, G50-70, G50-80, G50-80Touch
  - Lenovo Edge 15
  - Miix-Series: Miix2 – 8, Miix2 – 10, Miix2 – 11, Miix 3 - 1030
  - S-Series: S310, S410, S415, S415 Touch, S435, S20-30, S20-30 Touch, S40-70
  - U-Series: U330P, U430P, U330 Touch, U430 Touch, U540 Touch
  - Y-Series: Y430P, Y40-70, Y40-80, Y50-70, Y70-70
  - Yoga-Series: Yoga2-11, Yoga2-13, Yoga2Pro-13, Yoga3 Pro
  - Z-Series: Z40-70, Z40-75, Z50-70, Z50-75, Z70-80

Overview:

Recently security researchers have discovered a software known as Superfish pre-installed in Lenovo laptops. The Superfish technology is meant to help users find and discover products visually and instantly by analysing images on the web and presenting identical and similar product offers that may have lower prices. But what it ends up in serving unwanted adverts on web pages. This kind of software is called adware and represents a security risk as the software

also includes a proxy - a component that intercepts network traffic outside your browser so that it can keep track of what users are doing. Thus, if Superfish software is installed, it will monitor the websites you visit, and its contents, it can keep its eye out for related sites, all based on images instead of relying on old-fashioned keywords. This security issue could also be exploited to conduct attacks. Superfish make use of a man-in-the-middle proxy component to interfere with encrypted HTTPS connections, undermining the trust between users and websites. It was also found that Superfish relied on a third-party component for the HTTPS interception functionality: an SDK (software development kit) called the SSL Decoder/Digestor made by an Israeli company called Komodia. Komodia Redirector with SSL Digestor installs non-unique root Certificate Authority (CA) certificates and private keys which can allow attackers to conduct HTTPS spoofing.

Description

Komodia Redirector SDK is a self-described "interception engine" which is designed to allow developers to add proxy services and web traffic changes such as ad injection into their applications. With the SSL Digestor module, HTTPS traffic can also be manipulated. This is done by installing a root CA certificate into browser trusted certificate stores, allowing the proxy to act as man-in-the-middle and monitor all the web traffic without raising any flags for the end user.

In several applications implementing Komodia's libraries, such as Superfish Visual Discovery and KeepMyFamilySecure, the root CA certificates have been found to use trivially accessible, publicly disclosed, hard-coded private keys. It is to be noted that these keys seem to be different per application, though the same methods have proven successful in revealing the private keys in each instance.

It has also been found that besides sharing root CA certificates across installation, the SSL validation that Komodia itself performs is broken. This vulnerability can allow an attacker to attack all installations of Komodia Redirector, instead of focusing on a single application or certificate.

Solution

1. To check whether their systems contain Superfish and other Komodia root certificates, users can perform the Superfish Vulnerability Test, available on CERT-MU website: www.cert-mu.org.mu

2. If Superfish flaw is detected, users can uninstall any software that includes the Komodia Redirector and SSL Digestor libraries. An automated removal tool to uninstall Superfish is available on CERT-MU website: www.cert-mu.org.mu

3. Note that the names of these certificates are likely to vary based on the originating application. Microsoft provides guidance on deleting and managing certificates in the Windows certificate store, available on:

   https://technet.microsoft.com/en-us/library/cc772354.aspx
   http://windows.microsoft.com/en-us/windows-vista/view-or-manage-your-certificates

4. Mozilla provides similar guidance for their software, including the Firefox and Thunderbird certificate stores. More information is available on:

   https://wiki.mozilla.org/CA:UserCertDB#Deleting_a_Root_Certificate

Vendor Information

Lenovo

References

Lenovo
http://support.lenovo.com/us/en/product_security/superfish
http://news.lenovo.com/article_display.cfm?article_id=1929
https://forums.lenovo.com/t5/Lenovo-P-Y-and-Z-series/Lenovo-Pre-instaling-adware-spam-Superfish-powerd-by/m-p/1863174#M79882
http://news.lenovo.com/article_display.cfm?article_id=1929&cid=ww:social:147924660:147924659:TWITTER:lenovo:*%20Customer%20Service%20and%20Support&linkId=12450493
http://support.lenovo.com/us/en/product_security/superfish_uninstall

Microsoft
https://technet.microsoft.com/en-us/library/cc772354.aspx
http://windows.microsoft.com/en-us/windows-vista/view-or-manage-your-certificates

Security Tracker

Mozilla

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : contact@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu