Systems Affected

Lenovo consumer PCs that have Superfish VisualDiscovery installed.

Overview

Superfish adware installed on some Lenovo PCs install a non-unique trusted root certification authority (CA) certificate, allowing an attacker to spoof HTTPS traffic.

Description

Starting in September 2014, Lenovo pre-installed Superfish VisualDiscovery spyware on some of their PCs. This software intercepts users' web traffic to provide targeted advertisements. In order to intercept encrypted connections (those using HTTPS), the software installs a trusted root CA certificate for Superfish. All browser-based encrypted traffic to the Internet is intercepted, decrypted, and re-encrypted to the user's browser by the application – a classic man-in-the-middle attack. Because the certificates used by Superfish are signed by the CA installed by the software, the browser will not display any warnings that the traffic is being tampered with. Since the private key can easily be recovered from the Superfish software, an attacker can generate a certificate for any website that will be trusted by a system with the Superfish software installed. This means websites, such as banking and email, can be spoofed without a warning from the browser.

Although Lenovo has stated(link is external) they have discontinued the practice of pre-installing Superfish VisualDiscovery, the systems that came with the software already installed will continue to be vulnerable until corrective actions have been taken.

To detect a system with Superfish installed, look for a HTTP GET request to:

superfish.aistcdn.com

The full request will look like:

http://superfish.aistcdn.com/set.php?ID=[GUID]&Action=[ACTION]

Where [ACTION] is at least 1, 2, or 3. 1 and then 2 are sent when a computer is turned on. 3 is sent when a computer is turned off.

Superfish uses a vulnerable SSL decryption library by Komodia. Other applications that use the library may be similarly affected. Please refer to CERTVulnerability Note VU#529496 for more details and updates.

Impact

A machine with Superfish VisualDiscovery installed will be vulnerable to SSL spoofing attacks without a warning from the browser.

Solution

Uninstall Superfish VisualDiscovery and associated root CA certificate

Users should uninstall Superfish VisualDiscovery. Lenovo has provided a tool to uninstall Superfish (link is external)and remove all associated certificates.

It is also necessary to remove affected root CA certificates. Simply uninstalling the software does not remove the certificate. Microsoft provides guidance on deleting(link is external) and managing certificates(link is external) in the Windows certificate store. In the case of Superfish VisualDiscovery, the offending trusted root certification authority certificate is issued to "Superfish, Inc."

Mozilla provides similar guidance for their software, including the Firefox and Thunderbird certificate stores.

References

- [1] Lenovo Statement on Superfish(link is external)
- [2] CERT VU#529496
- [3] Delete a Certificate(link is external)
- [4] View or Manage a Certificate(link is external)
- [5] Deleting a root certificate
- [6] Lenovo Superfish Uninstall Instructions(link is external)

Revisions

- February 20, 2015: Initial release
- February 20, 2015: Clarified software release dates
- February 24, 2015: Updated description and solution details