FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security

Software used to deliver ads compromised web security features

Share This Page

FOR RELEASE

September 5, 2017

TAGS: Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Data Security

Note: *A conference call for media with FTC Acting Chairman Maureen K. Ohlhausen and Acting Director of the Bureau of Consumer Protection Tom Pahl will occur as follows:*
Date: September 5, 2017
Time: 11 a.m. ET
Call-in: (800) 230-1092; confirmation number 429578
Call-in lines, which are for ***media only****, will open 15 minutes prior to the start of the call. FTC staff will be available to take questions from the media.*

Lenovo Inc., one of the world's largest computer manufacturers, has agreed to settle charges by the Federal Trade Commission and 32 State Attorneys General that the company harmed consumers by pre-loading software on some laptops that compromised security protections in order to deliver ads to consumers.

In its complaint, the FTC charged that beginning in August 2014 Lenovo began selling consumer laptops in the United States that came with a preinstalled "man-in-the-middle" software program called VisualDiscovery that interfered with how a user's browser interacted with websites and created serious security vulnerabilities.

"Lenovo compromised consumers' privacy when it preloaded software that could access consumers' sensitive information without adequate notice or consent to its use," said Acting FTC Chairman Maureen K. Ohlhausen. "This conduct is even more serious because the software compromised online security protections that consumers rely on."

VisualDiscovery software, developed by a company called Superfish, Inc., was installed on hundreds of thousands of Lenovo laptops. It delivered pop-up ads from the company's retail partners whenever a user's cursor hovered over a similar looking product on a website.

To deliver its ads, VisualDiscovery acted as a "man-in-the-middle" between consumers' browsers and the websites they visited, even those websites that were encrypted. Without the consumer's knowledge or consent, this "man-in-the-

middle" technique allowed VisualDiscovery to access all of a consumer's sensitive personal information transmitted over the Internet, including login credentials, Social Security numbers, medical information, and financial and payment information. While VisualDiscovery collected and transmitted to Superfish's servers more limited information, such as the websites the user browsed and the consumer's IP address, Superfish had the ability to collect more information.

To facilitate its display of pop-up ads on encrypted websites (those that include https:// in the web address), the complaint also alleges that VisualDiscovery used an insecure method to replace digital certificates for those websites with its own VisualDiscovery-signed certificates. Digital certificates are used to signal to a user's browser that the encrypted websites visited by a consumer are authentic and not imposters. VisualDiscovery, however, did not adequately verify that the websites' digital certificates were valid before replacing them, and used the same, easy-to-crack password on all affected laptops rather than using unique passwords for each laptop.

Because of these security vulnerabilities, consumers' browsers could not warn users when they visited potentially spoofed or malicious websites with invalid digital certificates. The vulnerabilities also enabled potential attackers to intercept consumers' electronic communications with any website, including financial institutions and medical providers, by simply cracking the pre-installed password. The complaint alleges that Lenovo did not discover these security vulnerabilities because it failed to assess and address security risks created by third-party software it preloaded on its laptops.

As part of the settlement with the FTC, Lenovo is prohibited from misrepresenting any features of software preloaded on laptops that will inject advertising into consumers' Internet browsing sessions or transmit sensitive consumer information to third parties. The company must also get consumers' affirmative consent before pre-installing this type of software. In addition, the company is required for 20 years to implement a comprehensive software security program for most consumer software preloaded on its laptops. The security program will also be subject to third-party audits.

The Commission vote to issue the administrative complaint and to accept the consent agreement was 2-0. Acting Chairman Ohlhausen issued a statement on the case, and Commissioner Terrell McSweeny issued a concurring statement on the case.

The FTC will publish a description of the consent agreement package in the Federal Register shortly. The agreement will be subject to public comment for 30 days, beginning today and continuing through October 5, 2017, after which the Commission will decide whether to make the proposed consent order final. Interested parties can submit comments electronically by following the instructions in the "Invitation To Comment" part of the "Supplementary Information" section.

NOTE: The Commission issues an administrative complaint when it has "reason to believe" that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of up to $40,654.

The Federal Trade Commission works to promote competition, and protect and educate consumers. You can learn more about consumer topics and file a consumer complaint online or by calling 1-877-FTC-HELP (382-4357). Like the FTC on Facebook, follow us on Twitter, read our blogs and subscribe to press releases for the latest FTC news and resources.

Contact Information

MEDIA CONTACT:
Juliana Gruenwald Henderson,
Office of Public Affairs
202-326-2924

STAFF CONTACTS:
Linda Holleran Kopp,

Bureau of Consumer Protection
202-326-2267

Tiffany George,
Bureau of Consumer Protection
202- 326-3040