

DATE: March 03, 2015



TO: Tom Neff, Project Director  
US Army CHES (PEO-EIS)  
9351 Hall Road, Bldg. 1456  
Fort Belvoir, VA 22060

SUBJECT: Superfish Update

Mr.Neff:

Beginning in September 2014, Lenovo made a decision to ship some of our consumer notebooks with Superfish. This software frustrated some users without adding value to the experience. We began the process of removing it from our preloads. However, published reports about a security vulnerability created by this software were brought to our attention. Lenovo has now taken immediate action to remove it. Clearly this issue has caused concern among our customers, partners and those who care about Lenovo, our industry and technology in general. For this, I would like to apologize. I want to start the process of keeping you up to date on how we are working to fix the problem and restore your faith in Lenovo.

Lenovo has already taken several critical first steps:

- We stopped the preloads and will not include the Superfish software in any devices in the future.
- We have worked on our own and with our partners to make your PCs safe from this vulnerability as quickly and easily as possible:
  - On Thursday, Feb. 19, Lenovo provided a manual fix and by Friday, Feb. 20, we provided an automated removal tool to make it simple for our customers to remove Superfish and related files.
  - On Friday, Feb. 20, our partners, Microsoft, McAfee and Symantec updated their software to automatically disable and remove this Superfish software. This means users with any of these products active will be automatically protected. We thank them for their quick response.
  - Together, these actions mean all new products already in inventory will be protected. Shortly after the system is first powered-on the AV program will initiate a scan and then remove Superfish from the system. For systems which are re-imaged from the backup partition on the HDD, Superfish will also be removed in the same manner. For products already in use, Superfish will be removed when their antivirus programs update are initiated.

FROM: 1009 ThinkPlace  
Morrisville, NC 27560

[www.lenovo.com](http://www.lenovo.com)



We have communicated as rapidly as possible with customers, partners and industry watchers and influencers. I hope that with every communication, we are better informed and more clear on what is important.

Currently we are in the midst of developing a concrete plan to address software vulnerabilities and security with defined actions that we will share with everyone within the next few weeks. What I can say about this today is that we are exploring a wide range of options that include:

- Creating a cleaner PC image (We are starting immediately, and by the time we launch our Windows 10 products, our standard image will only include the operating system and related software, software required to make hardware work well (for example, when we include unique hardware in our devices, like a 3D camera), security software and Lenovo applications.)
- Offering Lenovo PC users affected by this issue a free 6 month subscription to McAfee's LiveSafe service (or a 6 month extension for existing subscribers). This information will be posted on [Lenovo.com](http://Lenovo.com).
- Working directly with users, privacy/security experts and others to create the right preload strategy quickly; and soliciting and assessing the opinions of even our harshest critics in evaluating our products going-forward.
- Posting information about ALL software we preload on our PCs that clearly explains what each application does.

While this issue was limited to our consumer notebooks, in no way did this matter impact the product models we sell through the CHES contract. Lenovo never installed the Superfish software on any Think Pad notebooks, nor any desktops, tablets, smartphones or servers and is no longer being installed on any Lenovo devices. We recognize that all Lenovo customers may have an interest in where we are and what is next. The fact is our reputation touches all of these areas, and all of our customers. Now, we are determined to make this situation better, deliver safer and more secure products and help our industry address – and prevent – the kind of vulnerabilities that were exposed in the last week

Thank you,

Gerald Fralick  
Deputy Chief Security Officer  
Office: 919-257-6172 • Cell: 919-801-9220 • Email: [gfralick@lenovo.com](mailto:gfralick@lenovo.com)

FROM: 1009 ThinkPlace  
Morrisville, NC 27560

[www.lenovo.com](http://www.lenovo.com)