Synaptics TouchPad Driver – Security Brief

Dec 14, 2017

By Synaptics Incorporated

(revision 1.2)

Synaptics provides TouchPads for notebook PC products, including the software driver that is needed to deliver a best-in-class usability experience. Synaptics takes our customer's security and privacy seriously, and we strive to meet or exceed industry best practices through continuous improvement.

Synaptics is aware of articles that were published where it was purported that there was a "keylogger" in our touchpad drivers. This is inaccurate. Our debug tool was mischaracterized in the articles as "keylogger".

Each notebook OEM implements custom TouchPad features to deliver differentiation. We have been working with these OEMs to improve the quality of these drivers. To support these requirements and to improve the quality of the experience, Synaptics provides a custom debug tool in the driver to assist in the diagnostic, debug and tuning of the TouchPad. This debug feature is a standard tool in all Synaptics drivers across PC OEMs and is currently present in production versions. This debug tool was turned off after production and prior to shipment. Synaptics believes now, for best industry practices, that it should remove this debug tool for production versions of the driver. Synaptics is unaware of any breach of security related to this debug tool.

After shipment, the supplier or user may wish to further tune and enhance the TouchPad experience by enabling the debug tool. The debug tool cannot be turned on or used except by a person with Admin access and special developer tools. When turned on, the debug tool collects data in a proprietary binary format for a rolling memory buffer that gets either overwritten or deleted every time a power event happens.

Using a standardized risk scoring system, the Common Vulnerability Scoring System (CVSS), this debug tool scores approximately 2 out of 10, and is classified as a low risk. In today's heightened sensitivity to security and privacy, Synaptics will take the precautionary steps of defeaturing the debug tool for production drivers to further prevent the tool from being used in an unintended and malicious way.

Synaptics is working closely with our PC customers to update drivers and to deploy them to address security concerns. Synaptics also recommends using best practices by restricting Admin access to any system as anyone with this level of access can potentially install malware or other anti-privacy software irrespective of whether the debug tool is on or off.

Synaptics takes great pride in making sure that its TouchPad drivers and other products meet industry-best security standards. In our new normal of heightened concern for security and privacy, Synaptics would like to apologize for any concerns that our debug tool may have raised. We have a path to immediately address this issue and other security concerns should they arise.

For more information, please review our Q&A.

If you have further questions, please contact David Hurd at dhurd@synaptics.com.

Partner Updates

Our Partner HP has made updates available in their Security Bulletin and driver updates are available for automatic installation on Microsoft's Windows Update Service.

For more details:

Synaptics Touchpad Driver: Potential, Local, Loss of Confidentiality

Release date: 2017-12-12

Potential Security Impact:

Potential, local, loss of confidentiality.

Source: Synaptics

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with certain versions of Synaptics touchpad drivers that can impact TouchPad models that use those drivers. A party would need administrative privileges and multiple accesses to the system in order to take advantage of the

vulnerability. Neither Synaptics nor our OEM customers have access to end-user data as a result of this issue.

Reference Numbers

CVE-2017-17556

BACKGROUND

CVSS 3.0 Base Metrics

Reference	Base Vector	Base Score
CVE-2017-17556	AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N	1.8