December 14, 2017 Version 1.0

Synaptics TouchPad Software Driver Q&A

- **What has been announced by reporters about Synaptics TouchPad™ software driver security?**
  - Some researchers have published reports about potential security vulnerabilities in some of Synaptics TouchPad software drivers. Synaptics is unaware of any breach of security related to this debug tool.

- **What is the function of Synaptics' TouchPad software driver?**
  - Synaptics provides complete TouchPad solutions for notebook PCs, including the software drivers used to deliver a best-in-class usability experience.

- **What is the claimed vulnerability?**
  - Synaptics provides a custom debug tool in the driver to assist OEMs in the diagnostic, debug and tuning of the TouchPad prior to production. This debug tool is then turned off for production, however, it can be turned on after production by someone with administrative privileges in order to continue to tune and enhance the experience. In order to exploit this vulnerability, a party would need to have both administrative privileges as well as knowledge of the proprietary procedure to enable it. By following best security practices such as making sure no one else uses your computer, this vulnerability can be mitigated until drivers can be updated.

- **Is there an official Synaptics communication about this issue?**
  - Yes, Synaptics has published a Security Brief on its corporate website. You can access it at this link: https://www.synaptics.com/company/blog/touchpad-security-brief

- **What are the effects of this vulnerability?**
  - If this debug tool is turned on by a user with Admin rights, the tool provides data to a small temporary rolling memory buffer that overwrites itself and gets erased every time a power event happens. The purpose of this tool is to assist in the diagnostic, debug and tuning of the TouchPad. The debug tool does not create a keylogger or text file. The data format is in a proprietary binary format.

- **What PC models are affected as a result of this vulnerability?**
  - Synaptics is preparing a full list of products that may be affected. Please note there are some classes of TouchPad products not affected at all. We advise users to look for updates to the Synaptics advisory page for the latest information.

- **How can users with impacted systems mitigate the vulnerabilities?**
    - Synaptics recommends that until new drivers become available, that users follow best security practices: this vulnerability can only be exploited by someone with administrative privileges to the PC.

- **When will new drivers be available for previously shipped systems?**
    - Synaptics is working closely with its partners to identify which products may be impacted and to promptly qualify new drivers, which will be available on Windows Update and on our partners websites.

- **What is the remedy to this vulnerability?**
    - Synaptics has taken the precautionary steps of defeaturing the debug tool for production drivers in order to prevent the tool from being used in an unintended and malicious way. Synaptics is working with PC customers to identify which products are impacted and to promptly qualify new drivers. Synaptics also recommends best practices by restricting Admin access to any system as it allows anyone with that level of access to potentially install malware or other anti-privacy software, irrespective of whether the debug tool is on or off.