Synaptics Security Advisory

Synaptics TouchPad Driver – SynTP.sys can leak freed pointers to kernel memory.

CVE: CVE-2018-15532

CVSS: 3.8 AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

Affected Drivers

File Description: Synaptics Pointing Device Driver

File Versions: All versions prior to 6/6/2018. Drivers since that date no longer have this vulnerability.

Impact

Synaptics' TouchPad Windows driver can leak freed kernel memory pointers. This could be used by an attacker to weaken KASLR (see below).

Background

SynTP.sys is a driver that controls Synaptics' TouchPad families of products on Windows. It exposes an API used to control the features of the device.

Technical Details

Invalidly formatted API requests can cause SynTP.sys to reveal freed kernel memory pointers.

As the revealed data is no longer in use, the confidentiality impact is indirect and unpredictable, and therefore categorized in the CVSS score as Low.

However, if the driver is not updated, these pointers could be used to analyze patterns of kernel memory that has been previously used. This weakens the protections of Window's Kernel Address Space Layout Randomization, a technique that makes it more difficult to exploit vulnerabilities in access to kernel memory. An attacker could more easily find kernel memory locations to examine if they could somehow obtain access to kernel memory.

Acknowledgements

Synaptics would like to thank Enrique Nissim, Senior Security Consultant for IOActive, Inc., for reporting this issue.