



CVE-2018-15532

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-15532
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:00:00 UTC
Updated	2019-03-27 17:55:00 UTC
Description	SynTP.sys in Synaptics Touchpad drivers before 2018-06-06 allows local users to obtain sensitive information about freed I

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Synaptics Touchpad Driver	All	All	All	All

References

Reference	Source	Link	Tags
Synaptics TouchPad 'SynTP.sys' Local Information Disclosure Vulnerability	MISC	www.securityfocus.com	Third Party Adviso
Synaptics Touchpad Driver Leaks Kernel Memory Pointers - Lenovo Support US	MISC	support.lenovo.com	Third Party Adviso
www.synaptics.com/sites/default/files/touchpad-driver-security-brief-20190124.pdf	CONFIRM	www.synaptics.com	Vendor Advisory
TouchPad Solutions for Notebooks Synaptics	MISC	www.synaptics.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)