



# CVE-2017-9769

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

## Summary

<b>CVE</b>	CVE-2017-9769
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-08-02 19:29:00 UTC
<b>Updated</b>	2020-05-28 19:13:00 UTC
<b>Description</b>	A specially crafted IOCTL can be issued to the rzpnk.sys driver in Razer Synapse 2.20.15.1104 that is forwarded to ZwOpen

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Razer</a>	<a href="#">Synapse</a>	2.20.15.1104	All	All	All
Application	<a href="#">Razer</a>	<a href="#">Synapse</a>	2.20.15.1104	All	All	All

## References

Reference	Source	Link
Razer Synapse rzpnk.sys ZwOpenProcess   Rapid7	MISC	<a href="http://www.rapid7.com">www.rapid7.com</a>
Razer Synapse 2.20.15.1104 - rzpnk.sys ZwOpenProcess (Metasploit) - Windows_x86-64 local Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>
Razer rzpnk.sys IOCTL 0x22a050 ZwOpenProcess (CVE-2017-9769)   War Room	MISC	<a href="http://warroom.securestate.com">warroom.securestate.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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](#).

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