



# CVE-2019-11419

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

## Summary

<b>CVE</b>	CVE-2019-11419
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-05-14 19:29:00 UTC
<b>Updated</b>	2023-03-01 15:29:00 UTC
<b>Description</b>	vcodec2_hls_filter in libvoipCodec_v7a.so in the WeChat application through 7.0.3 for Android allows attackers to cause a c

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tencent	Wechat	All	All	All	All

## References

Reference	Source	Link	Tags
DoS Wechat with an emoji - Home	MISC	<a href="https://awakened1712.github.io">awakened1712.github.io</a>	Exploit, Technical Description
WeChat for Android 7.0.4 - 'vcodec2_hls_filter' Denial of Service	EXPLOIT-DB	<a href="https://www.exploit-db.com">www.exploit-db.com</a>	
WeChat 7.0.4 Denial Of Service ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#)**