



CVE-2021-31584

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

Summary

CVE	CVE-2021-31584
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-23 21:15:00 UTC
Updated	2022-07-30 03:45:00 UTC
Description	Sipwise C5 NGCP www_csc version 3.6.4 up to and including platform NGCP CE mr3.8.13 allows call/click2dial CSRF atta

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sipwise	C5	3.6.7	All	All	All
Application	Sipwise	Next Generation Communications Platform	3.6.7	All	All	All
Application	Sipwise	Next Generation Communication Platform	3.6.4	All	All	All

References

Reference	Source	Link	Tags
Sipwise - Enjoy a new future in the cloud with Unified Communications	MISC	www.sipwise.com	
Sipwise C5 NGCP CSC Cross Site Request Forgery ≈ Packet Storm	MISC	packetstormsecurity.com	
[Spce-user] About CVE-2021-31583 and CVE-2021-31584	MISC	lists.sipwise.com	
Zero Science Lab	MISC	www.zeroscience.mk	
Zero Science Lab » Sipwise C5 NGCP CSC CSRF Click2Dial Exploit	MISC	www.zeroscience.mk	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)