Sipwise C5 NGCP CSC Multiple Stored/Reflected XSS Vulnerabilities

Title: Sipwise C5 NGCP CSC Multiple Stored/Reflected XSS Vulnerabilities
Advisory ID: ZSL-2021-5648
Type: Local/Remote
Impact: Cross-Site Scripting
Risk: (3/5)
Release Date: 23.04.2021

Summary

Sipwise C5 (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.

Description

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.

Vendor

Sipwise GmbH - https://www.sipwise.com

Affected Version

<=CE_mr9.3.1
NGCP www_admin version 3.6.7

Tested On

Apache/2.2.22 (Debian)
Apache/2.2.16 (Debian)
nginx

Vendor Status

[13.04.2021] Vulnerability discovered.
[19.04.2021] Contact with the vendor.
[22.04.2021] No response from the vendor.
[23.04.2021] Public security advisory released.
[26.04.2021] Vendor responds with clarification of vulnerable versions and working on fixes.
[26.04.2021] NGCP www_admin version 3.6.7 has not been in use since mr3.0, 7+ years ago, and that component has been completely abandoned around 4 years ago: https://github.com/sipwise/www_admin/
[26.04.2021] The 'addressbook' is distinct from the 'phonebook' and was available only on www_csc, which has not been used for 7 years now.

PoC

sipwise_xss.txt

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31583
[2] https://nvd.nist.gov/vuln/detail/CVE-2021-31583
[3] https://www.exploit-db.com/exploits/49800
[4] https://packetstormsecurity.com/files/162316
[5] https://cxsecurity.com/issue/WLB-2021040136
[6] https://exchange.xforce.ibmcloud.com/vulnerabilities/200605
[7] https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2021-31583

Changelog

[23.04.2021] - Initial release
[25.04.2021] - Added reference [5], [6] and [7]
[06.05.2021] - Added vendor status

Contact

Zero Science Lab

Web: https://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- **Profiles**

-