[Spce-user] About CVE-2021-31583 and CVE-2021-31584

Guillem Jover gjover at sipwise.com
Thu Sep 2 14:46:40 EDT 2021

```
Hi!

In case someone has noticed these CVEs that were issued some months ago,
here is some clarification to give some peace of mind regarding the
affected components and releases we have been trying to get the reporter
to update (since May), but unfortunately that has not yet happened. I'll
be directly requesting Mitre to update the information in the advisories.


* CVE-2021-31583 / ZSL-2021-5648

  AKA "Sipwise C5 NGCP CSC Multiple Stored/Reflected XSS Vulnerabilities"

  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31583
  https://nvd.nist.gov/vuln/detail/CVE-2021-31583
  https://www.zeroscience.mk/en/vulnerabilities/ZSL-2021-5648.php

  The title should be "NGCP WWW Admin" instead of "NGCP CSC".

  The affected version should be:

    NGCP www_admin version 3.6.7
    <= NGCP CE 3.0 (up to and including)

* CVE-2021-31584 / ZSL-2021-5649

  AKA "Sipwise C5 NGCP CSC CSRF Click2Dial Exploit"

  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31584
  https://nvd.nist.gov/vuln/detail/CVE-2021-31584
  https://www.zeroscience.mk/en/vulnerabilities/ZSL-2021-5649.php

  The affected version should be:

    NGCP www_csc version 3.6.4
    <= NGCP CE mr3.8.13 (up to and including)


Both only affected long unsupported NGCP releases.

Thanks,
Guillem
```

[More information about the Spce-user mailing list](#)