

# Exploitation of Control Web Panel CVE-2022-44877

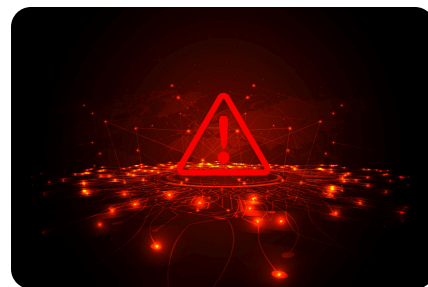
Jan 19, 2023 | 1 min read |

Caitlin Condon



*Last updated at Fri, 20 Jan 2023  
14:52:20 GMT*

On January 3, 2023, security researcher Numan Türle [published](#) a proof-of-concept exploit for CVE-2022-44877, an unauthenticated remote code execution vulnerability in Control Web Panel (CWP, formerly known as CentOS Web



## Topics

Metasploit (653)

Vulnerability  
Management (359)

Research (236)

Detection and Response  
(205)

Vulnerability Disclosure  
(148)

Emergent Threat  
Response (141)

Cloud Security (136)

Security Operations (20)

## Popular Tags

Contact Us

condition that allows attackers to run bash commands when double quotes are used to log incorrect entries to the system. Successful exploitation allows remote attackers to execute arbitrary operating system commands via shell metacharacters in the login parameter (`login/index.php`).

On January 6, 2023, security nonprofit Shadowserver [reported](#) exploitation in the wild. As of January 19, 2023, security firm GreyNoise has also seen several IP addresses [exploiting CVE-2022-44877](#) [↗](#).

Control Web Panel is a popular free interface for managing web servers; Shadowserver's

Metasploit

Metasploit Weekly  
Wrapup

Vulnerability  
Management

Research

Logentries

Detection and Response



Related Posts

Fortinet  
FortiManager CVE-  
2024-47575  
Exploited in Zero-  
Day Attacks [READ](#)  
[MORE](#)

Multiple  
Vulnerabilities in  
Common Unix  
Printing System  
(CUPS) [READ](#)  
[MORE](#)

High-Risk  
Vulnerabilities in

Contact Us

appear to be a detailed vendor advisory for CVE-2022-44887, but available information indicates Control Web Panel 7 (CWP 7) versions before [0.9.8.1147](#)  are [vulnerable](#) .

CWP users should upgrade their versions to 0.9.8.1147 or later as soon as possible.

# Rapid7 customers

## InsightVM & Nexpose

**customers:** An authenticated vulnerability check for CVE-2022-44877 was made available in the January 19 content release.

CVE-2024-40700.  
Critical Improper  
Access Control  
Vulnerability  
Affecting SonicWall [READ](#)  
Devices [MORE](#)

## POST TAGS

Contact Us



## AUTHOR

### Caitlin Condon

Director, Vulnerability  
Intelligence

[VIEW CAITLIN'S POSTS](#)

## Related Posts

#### EMERGENT THREAT RESPONSE

Fortinet FortiManager CVE-2024-47575  
Exploited in Zero-Day Attacks

#### EMERGENT THREAT RESPONSE

Multiple Vulnerabilities in Common Unix  
Printing System (CUPS)

Contact Us

**EMERGENT THREAT RESPONSE**  
High-Risk Vulnerabilities in Common Enterprise Technologies  
  
[READ FULL POST](#)

**EMERGENT THREAT RESPONSE**  
CVE-2024-40766: Critical Improper Access Control Vulnerability Affecting SonicWall Devices  
  
[READ FULL POST](#)

[VIEW ALL POSTS](#)



CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free)

SALES SUPPORT

+1-866-772-7437 (Toll Free)

Need to report an Escalation or a Breach?

 GET HELP

SOLUTIONS

The Command Platform




Exposure Command

Managed Threat Complete

SUPPORT & RESOURCES

ABOUT US

Contact Us



Select ▾

START TRIAL

Events & Webcasts

Training & Certification


Cybersecurity Fundamentals

Vulnerability & Exploit Database

News & Press Releases

Public Policy

Open Source


Investors 





CONNECT WITH US

Contact

Blog

Support Login

Careers 



Contact Us