



PROFILE

CVE-2022-44877

ZEROFOX INTELLIGENCE

P-2023-02-09a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Common Vulnerabilities & Exposures

February 9, 2023



Intelligence Cut-off: 12:00 PM (EST) on February 8, 2023

Metasploit Available: Yes



Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-78	Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection")	NIST

Vulnerability Analysis

CVE-2022-44877 is a RCE within CWP 7, which was responsibly disclosed and patched on October 25, 2022. The security researcher, Numan Türle, released his proof of concept on January 5, 2023,¹ via GitHub. A Metasploit module leveraging this vulnerability was subsequently uploaded to GitHub.

The simplicity of this exploit, along with an available Metasploit module, allows threat actors to scan for this vulnerability easily. Even months after a patch has been released for this vulnerability, threat actors are still looking for vulnerable systems. This active interest is shown in Figure 1; GreyNoise[.]io detected nine unique IP addresses attempting to exploit CVE-2022-44877 throughout the month of January 2023.

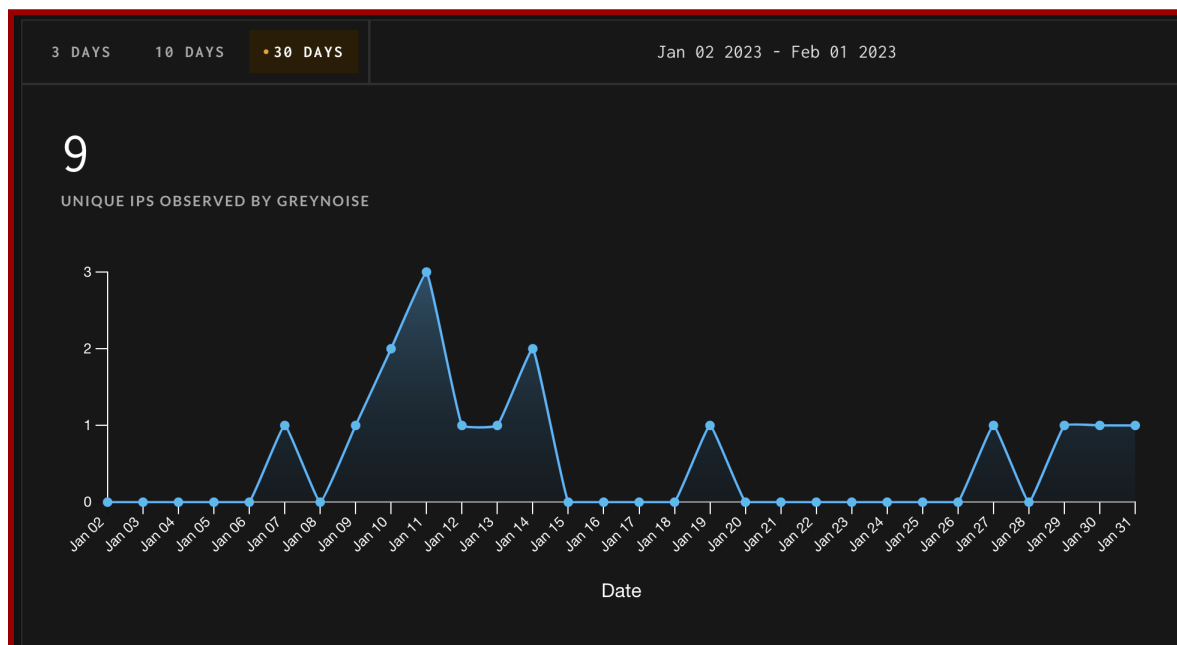


Figure 1. Unique IP Scanning for CVE-2022-44877 Over Time

Source: [hXXps://viz.greynoise\[.\]io/tag/centos-web-panel-rce-cve-2022-44877-attempt?days=30](https://viz.greynoise.io/tag/centos-web-panel-rce-cve-2022-44877-attempt?days=30)

CWP CVE-2022-44877 takes advantage of an OS command injection when making a request to *login.php*. The crux of the vulnerability stems from the logging functionality

¹ [hXXps://github\[.\]com/numanturle/CVE-2022-44877](https://github.com/numanturle/CVE-2022-44877)



found, with CWP relying on the bash *echo* command to print log entries. Since the logging functionality also records submitted URL parameters, a threat actor can abuse bash built-in features called Command Substitution to inject OS commands via URL parameters.

Recommendation

On October 25, 2022, a patch for CVE-2022-44877 was released; ZeroFox recommends updating to the latest version. If updating is not immediately possible, put this application behind a VPN, limiting its exposure to the internet. ZeroFox also recommends installing and configuring Filebeat to ingest CWP7 logs. On a CentOS 7 Installation, the logs can be located within the `/usr/local/cwpsrv/logs` folder.



Appendix 1: Indicators of Compromise (Sigma Rules)

```
title: CVE-2022-44877
id: da2cba21-3f18-4310-aaf3-e111c53bbe45
description: Sigma Rule to detect exploit attempts of CVE-2022-44877 a RCE vulnerability within
CWP7 <= .1146 and lower.
status: experimental
date: 2023/02/08
modified: 2023/02/08
author: ZeroFox
tags:
- mitre.T1190
- mitre.T1059
- attack.InitialAccess
- attack.Execution
references:
- https://nvd.nist.gov/vuln/detail/CVE-2022-44877
-
http://packetstormsecurity.com/files/170388/Control-Web-Panel-7-Remote-Code-Execution.html
-
http://packetstormsecurity.com/files/170820/Control-Web-Panel-Unauthenticated-Remote-Comm
and-Execution.html
- http://seclists.org/fulldisclosure/2023/Jan/1
- https://gist.github.com/numanturle/c1e82c47f4cba24cff214e904c227386
- https://www.youtube.com/watch?v=kiLfSvcISYY
logsource:
product: linux
detection:
selection:
  log.file.path: '*access_log'
  event.original:
    - '*/login/index.php?login=$(*)*'
condition: selection
level: high
```

Figure 2. Sigma Rules to detect CVE-2022-44877

Source: ZeroFox Intelligence Collections



Appendix 2: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.