Vulnerability advisory - CVE-2020-9368

Publisher

Oleacorner, through Prestashop's marketplace

Product

Prestashop module `Olea Gift On Order`

Title

Olea Gift On Order - Unauthenticated arbitrary file read

Publication date

November 2nd, 2020

Risk level

High

Exploitability

Remote

Impact

Technical information disclosure

Description

Olea Gift On Order module through 5.0.8 for PrestaShop enables an unauthenticated user to read arbitrary files on the server via `getfile.php?file=/..` directory traversal.

As there is no access control over the `getfile.php` page, any unauthenticated user can call this file in their browser to retrieve the content of any page in any (sub)folder of the Prestashop folder.
This is done by making a GET request to `getfile.php` with `file` parameter set to the file the user wants to retrieve.

The `_PS_ROOT_DIR` (root of the Prestashop folder) variable is prepended to the file being retrieved. However, as there is no filtering on the input passed in `file` GET parameter, by prepending several `../` a user can retrieve files outside of the Prestashop directory.

Affected versions

Versions <= 5.0.8 (latest)

Solutions

Manual removal of the `getfile.php` file as suggested by Oleacorner.
No patch will be provided by the publisher.

Credit

Vulnerability discovered by Florent BESNARD from INTRINSEC

History

2020-02-21: Oleacorner contacted via email
2020-02-22: Prestashop security team contacted via email
2020-02-24: Prestashop acknowledged the vulnerability. The module was removed from the marketplace and the publisher was notified. CVE-2020-9368 was assigned
2020-02-25: Oleacorner acknowledged the vulnerability and recommended the manual removal of the vulnerable file
2020-03-19: Intrinsec asked for updates from Oleacorner and Prestashop. No reply received
2020-06-22: Intrinsec asked for updates from Oleacorner. No reply received
2020-11-02: Advisory publication