

[Open in app](#)[Get started](#)

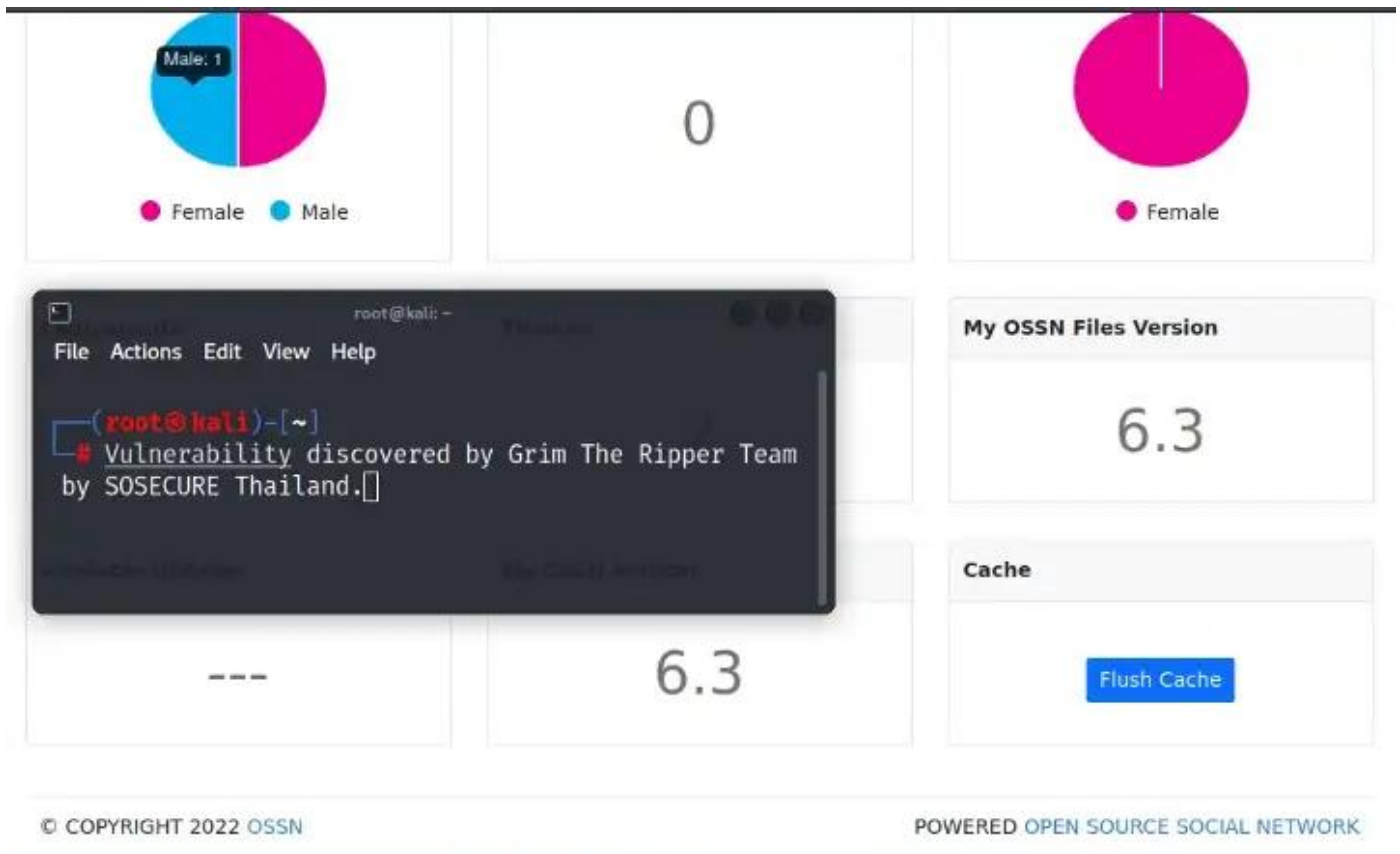
GrimTheRipper

[Follow](#)

Jul 8 · 3 min read · [Listen](#)

[Save](#)

[CVE-2022-34965] Open Source Social Network 6.3 LTS— Authenticated Unrestricted File Upload (Components)



Description

#OpenTeknik LLC OSSN OPEN SOURCE | 1 ORK v6.3 LTS was discovered to contain an arbitrary file upload vulnerability via the component `/ossn/administrator/com_installer`.





Open in app

Get started

Steps to attack:

First, we log in to the OSSN 6.3 as the admin privileges on the administrator page.

The screenshot shows a web browser window with the address bar displaying `/ossn/administrator`. The page features the "OPENSOURCE SOCIAL NETWORK" logo at the top. Below the logo is a section titled "ADMINISTRATION" containing a login form. The form has two input fields: "Username" with the text "admin" and "Password" with masked characters. A blue "Login" button is positioned below the password field. At the bottom of the page, there is a copyright notice "© COPYRIGHT 2022 OSSN" and the text "POWERED OPEN SOURCE SOCIAL NETWORK".

`http://<IP>/ossn/administrator`

And then we proceed towards to menu Components > installer

The screenshot shows the "COMPONENT INSTALLER" page in the OSSN administrator interface. The page has a dark header with the "OPENSOURCE SOCIAL NETWORK" logo and a navigation menu. The main content area is titled "COMPONENT INSTALLER" and contains a file upload section. It includes a "Browse..." button, the text "No file selected.", and a green "Upload" button. Below these elements is a light blue message box that reads "Upload a valid .zip component package.".



Open in app

Get started

The screenshot shows the OpenSource Social Network website. The header includes the site name, navigation links (Home, Hosting, Community, Developers, Download, Search), and a user profile (LABIW74728@MEIDIR.COM). The main content area displays a component titled 'Languages List' by Arsalan Shah, 3 months ago, with a 5.0 rating. The component description states: 'You can enable the languages you wish to display on user profile edit page. This will help you to disable the incomplete language packs.' Below the description is a list of available languages with checkboxes. To the right, a 'Component' sidebar shows details: Developer: Arsalan, License: ossnv4, Type: Tools, Requires Ossn Version: 6.0, Latest Version: 1.2, Last Updated: 3 months ago, and Repository Url: View Repository. Below this, a 'Versions' section shows download buttons for v1.2 and v1.1.

Languages List

Download 1.2

Arsalan Shah 3 months ago 5.0

You can enable the languages you wish to display on user profile edit page. This will help you to disable the incomplete language packs.

AVAILABLE LANGUAGES

You can enable the languages you wish to display on user profile edit page. This will help you to disable the incomplete language packs.

Comments

COMMENT

Component

Developer: Arsalan

License: ossnv4

Type: Tools

Requires Ossn Version : 6.0

Latest Version: 1.2

Last Updated: 3 months ago

Repository Url: View Repository

Versions

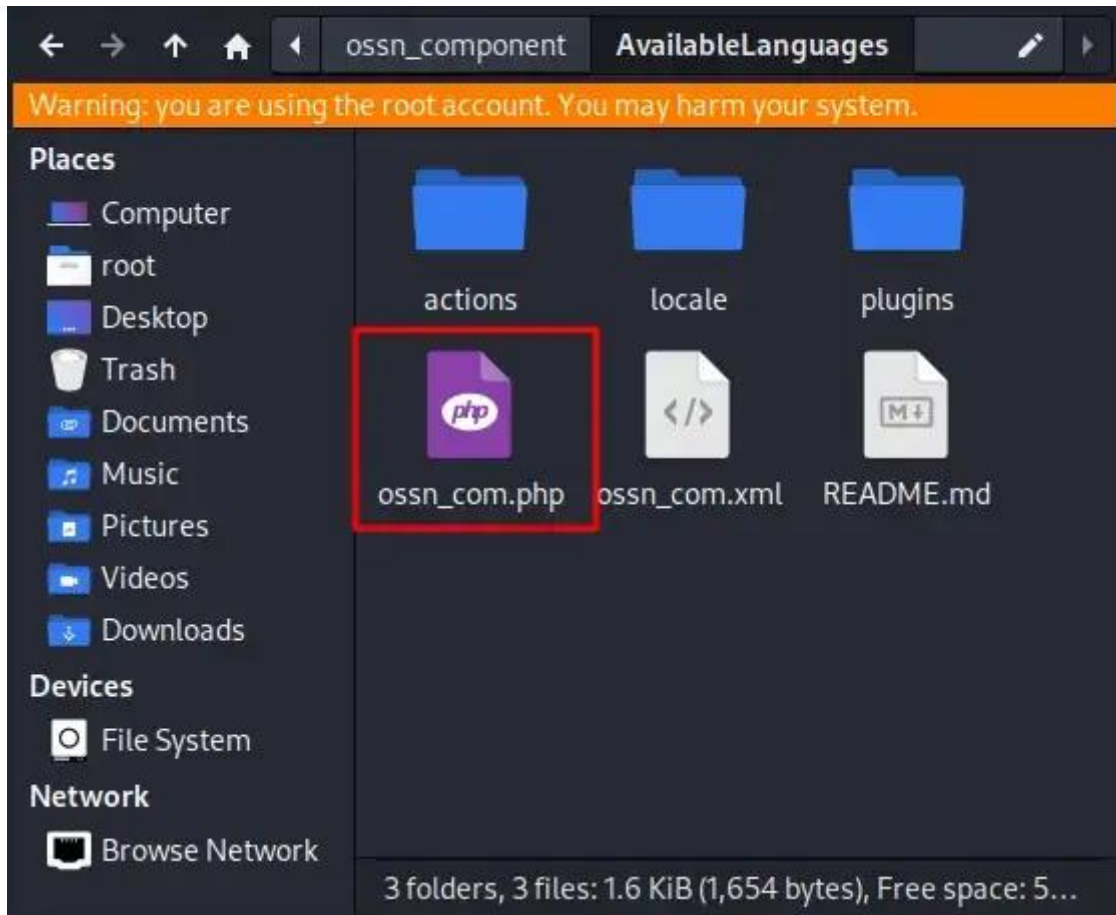
Download v1.2

Download v1.1

<https://www.opensource-socialnetwork.org/component/view/5909/languages-list>

When unzipping the theme that we download, we will find the `ossn_com.php` file in the directory of the theme.



[Open in app](#)[Get started](#)

It looks like we can change the content of the ossn_com.php file to PHP reverse shell.





Open in app

Get started

Edit content of ossn_com.php to PHP reverse shell.





[Open in app](#)

Get started

Create an archive in type zip that contains the directory of components.

Proceed towards to menu Components > installer and click on the Browse button.





Open in app

Get started

`http://<IP>/osn/administrator/com_installer`

Choose the archive that we create.

Choose the archive that we create.





Open in app

Get started

Now, our component with the malicious files is all ready to use.

Using netcat to listen for TCP connections on port 443.





Open in app

Get started

Direct access to ossn_com.php file that we edit the content to PHP reverse shell via the link following.

`http://<IP>/osn/components/AvailableLanguages/osn_com.php`

`http://<IP>/osn/components/AvailableLanguages/osn_com.php`

Bravo!, We get the system shell on the web server which uses Open Source Social Network 6.3.





Open in app

Get started

Discoverer:

Grim The Ripper Team by SOSECURE Thailand

Reference:

1. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34965>
2. <https://www.opensource-socialnetwork.org/>
3. <https://github.com/opensource-socialnetwork/opensource-socialnetwork/releases/tag/6.3>
4. <https://www.openteknik.com/contact?channel=ossn>





[Open in app](#)

[Get started](#)

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

