CVE-2022-25018 - RCE/OS Injection

February 25, 2022

1 Application

`https://github.com/pluxml/PluXml`

2 Introductory Remarks

There is already an issue regarding a different RCE vulnerability (`https://github.com/pluxml/PluXml/issues/321`). In contrast to our vulnerability, said RCE only works when using the config_file parameter with admin privileges, which is not possible as a moderator.

3 Description of the Vulnerability

In the PluXml PHP blogging platform (v5.8.7), a user with the manager role can inject arbitrary PHP code that is executed on the server. As a consequence, remote code execution (RCE) becomes possible, as illustrated in this unlisted (non-public) youtube video: `https://youtu.be/Gbe2UNCB0tY`.

4 Steps to Reproduce the Exploit

1. Login with a manager account.
2. In the Administration menu, select static pages and edit one of the pages.
3. Insert PHP code with starting and closing tags `<?php` *`CODE`* `?>`.
4. Save the changes and open the stored page.

5 Technical Description of the Vulnerability

While the administrator role has the permission to edit PHP templates and, thus, can always execute arbitrary code, the manager role has no such privileges. Indeed, a manager can only edit so-called static - purely HTML-written - pages. However, in the file `core/admin/statique.php` and in the file `core/admin/lib/class.plx.admin.php` (in the function `editStatique`) no proper input sanitisation is done to filter PHP-opening- and closing-tags (`<?php` and `?>`). As a consequence, the injected PHP code becomes executed on the server-side, even though it is integrated with HTML content. Additionally, note that an XSS-attack is also possible for a manager (proof of concept: by integrating `<script>alert(/xss/)</script>`) and hard to filter.