

Errata - 4.2.0 and earlier Javascript vulnerability

Javascript link creation vulnerability

Last revised: 2021-11-01

Summary

Unfortunately there is an issue with link creation in the GUI with Open-Audit Community.

If a bad value is passed to the routine via a URL, javascript code can be executed.

This requires the user be logged in to Open-Audit Community to trigger.

Severity: Medium

The conditions of successful exploitation are that the user clicking the bad URL be logged in to Open-Audit Community.

Products Affected

Open-Audit Community all versions.

Available Updates

A patch for the issue described in this bulletin will be available in the next released Open-Audit v4.3.0.

Workarounds and Mitigations

Download the attached file and replace the following file:

Linux - /usr/local/open-audit/code_igniter/application/helpers/output_helper.php

Windows - c:\xampp\open-audit\code_igniter\application\helpers\output_helper.php

The file is also available on Github at https://raw.githubusercontent.com/Opmantek/open-audit/master/code_igniter/application/helpers/output_helper.php

You can view the associated commits also on Github at:

<https://github.com/Opmantek/open-audit/commit/e37b64bbd0219f03cb71cc1cd5bb010166a2b846>

