

Errata - 4.2.0, 3.5.0 and onwards util function vulnerability

util function vulnerability

Last revised: 2021-11-01

Summary

A vulnerability has been reported in the utility controller used by Open-Audit. The vulnerability has been fixed and a patch is available as well as included in the next release of Open-Audit (4.3.0). The vulnerability is caused by un-validated user input to a publicly available function. The patch removes this vulnerability by validating the user input.

Severity: Severe

This issue is remotely exploitable by unauthenticated users. All users are advised to apply the patch immediately.

Products Affected

Open-Audit versions 3.5.0 and later.

Available Updates

A patch for the issue described in this bulletin will be available in the next released Open-Audit v4.3.0, expected before Nov 12th (subject to change).

Fixes, Workarounds and Mitigations

Download the attached file and replace the following file:

Linux - /usr/local/open-audit/code_igniter/application/controllers/util.php

Windows - c:\xampp\open-audit\code_igniter\application\controllers\util.php

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

You can see the code changed for this patch, also on Github at <https://github.com/Opmantek/open-audit/commit/1ce039306d85598880ff25fbeb20195ef3b7a993#diff-0d4f2e9612b02690fdeac430d36d1a8c334d6fb1e1d17c223cbfe5321b2bd04e>



util.php