
CVE-2014-3718: Cross Site Scripting in Aleph

- **Article Type:** Q&A
 - **Product:** Aleph
 - **Product Version:** 18
-

Question

We found the following security report CVE-2014-3718 regarding Aleph:

<http://packetstormsecurity.com/files/126654/Aleph-500-Cross-Site-Scripting.html> published on May 16, 2014.

Could you provide any information that you have related to this? Is this something that we should be concerned about?

Answer

Following our investigation by reproducing the vulnerabilities with an internal security vulnerability assessment tool, those vulnerabilities are fully fixed in Aleph version 22 (latest version). Our recommendation is to implement version 22.

Aleph OPAC (without using PDS) is not vulnerable if in \$alephe_tab/tab100 is set:

XSS-VALIDATION=Y

(V18 - rep_change #1503

V19 - rep_change #174

V20 - rep_ver #15191)

Customers using PDS may still be vulnerable if they are using Aleph versions lower than Aleph 22.

- **Article last edited:** 8/13/2014