HTTP Response Splitting Vulnerabilities

- **Product:** Aleph
- **Product Version:** 20, 21, 22, 23
- **Relevant for Installation Type:** Dedicated-Direct, Direct, Local, Total Care

Description

This nt.cgi issue showed up in the pentest from a few months ago. Now it's showing in the weekly vulnerability reports.

HTTP Response Splitting Vulnerabilities

Description
HTTP Response Splitting attacks occur when the server script embeds user data in HTTP response headers. Examples of this would be: a script embedding user data in the redirection URL of a redirection response, and a script embedding user data in a cookie value.

Consequence
As a result of the attack user data can become a part of the HTTP response headers, and can facilitate several attacks: cross-site scripting, web cache poisoning, hijacking pages with user-specific information, and browser cache poisoning.

Solution
Any data collected from the client should be URL-encode strings before inclusion into HTTP headers such as Location or Set-Cookie.

Detail Output
HTTP/1.1 200 OK Content-Type: text/html Set-Cookie: a=q Content-Length: 2 AA Please <A HREF="javascript:history.go(-1)">go back</A>and try again!

Payload
func=http://catalog.xxxx.edu:80/F/83P1LQ2

URI

...

Resolution

Aleph Development has checked this and writes: "We saw a directory /exlibris/aleph/u20_1//alephe/apache/cgi-bin (not cgibin) and under it a file new_titles.cgi (not nt.cgi). If indeed this fits (cgibin to cgi-bin etc...), then it does look as if these

URI are indeed custom-made."

"There is no cgi-bin or cgibin in the generic, as-delivered apache; it seems this is something which has been added locally.

If you want to pursue this problem, you will need to reproduce it with the generic, as-distributed apache (as seen in /exlibris/aleph/a20_1/alephe.orig/apache/).

- **Article last edited:** 16-Aug-2016