Apache vulnerability - CVE-2016-5387

- **Product:** Apache
- **Product Version:** 2.2.x and lower
- **Relevant for Installation Type:** All environments

Ex-Libris is aware of the new apache vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5387) which involves HTTP_PROXY header and CGI (as described in https://httpoxy.org/).

Several requirements must be fulfilled in order for an environment to be vulnerable:

- Code needs to be running under a CGI-like context, where HTTP_PROXY becomes a real or emulated environment variable
- An HTTP client that trusts HTTP_PROXY, and configures it as the proxy, must exist
- That client, used within a request handler, must be making an HTTP (as opposed to HTTPS) request

Our research found that:

- In products where code is running under CGI the Perl client (LWP::HTTP) does not use the HTTP_PROXY variable and is therefore considered of low risk.
- Products running apache tomcat are not running CGI.
- Other products have no access to the web and are therefore considered of low risk.

These conclusions are relevant only to code produced by Ex-Libris. CGI code installed by customers which was not supplied by ExLibris cannot be guaranteed to be safe.

While the risk level of this vulnerability is deemed as LOW for Ex-Libris products, once an official version with the relevant fix is announced by apache, our development team will build and implement it in future releases.

- **Article last edited:** 25-July-2016