Security vulnerability issues – Basic troubleshooter

- **Product:** Cross-Product

Description

The below troubleshooting steps are relevant if you encountered a security vulnerability by running a pro-active scan on your ExLibris applications or if you've encountered a new vulnerability via a different channel.
Vulnerabilities are security risks which may affect 3rd party products used by ExLibris applications.
Most vulnerabilities are marked with a CVE ID (For example: CVE-2015-3456), for information regarding a specific vulnerability we recommend checking specialized sites such as https://nvd.nist.gov/.

Resolution

In general, we recommend always upgrading 3rd-party products to the latest supported versions in order to make sure you are not vulnerable. This can be done using the **util sp** method (see this knowledge article for explanations on using **util sp** for upgrading 3rd-party products).

What to do when encountering a possible security vulnerability in an ExLibris product:

1. Check the Announcements section of the ExLibris Security Zone for announcements of new known vulnerability policies.
2. If the vulnerability is not mentioned in the security zone it might already be resolved in a supported version of the relevant 3rd party program.
    a. Find the vulnerability CVE ID in a specialized site, such as https://nvd.nist.gov/, and check in which version the vulnerability was resolved.
    b. Check the ExLibris Certified Third-Party Software and Security Patch Release Notes:
        i. If the version of the fix is supported by ExLibris – update the 3rd-party products using the **util sp** method; this should resolve the vulnerability issues (see this knowledge article for explanations on using **util sp** for upgrading 3rd-party products).
        ii. If the version of the fix is not yet supported by ExLibris or Util SP is not executable, and the vulnerability is not addressed in the ExLibris Security Zone (step #1) – please contact support via CRM, setting category to "security and privacy" + relvant sub-category, including the vulnerability CVE ID. The support analyst handling the case will forward your report to the ExLibris security officer for analysis. Please do not share this kind of information in mailing lists, forums or over the internet. Instead, please contact Ex Libris Support as described above so that the Ex Libris vulnerability analysis and escalation processes can be initiated (For more information, please see the ExLibris vulnerability analysis policy)
3. in any security or privacy issue, concern or question, please contact support via CRM, setting category to "security and privacy" + relvant sub-category. The support analyst handling the case will forward your report to the ExLibris security or privacy officer for analysis. . Please do not share this kind of information in mailing lists, forums or over the internet. Instead, please contact Ex Libris Support as described above so that the Ex Libris vulnerability analysis and escalation processes can be initiated.

Additional Information

More information on known vulnerabilities can be found at organizations such as National Vulnerability Database - https://nvd.nist.gov/.

- ExLibris Security Zone
- ExLibris Certified Third-Party Software and Security Patch Release Notes
- ExLibris New Third Party Software Evaluation and Plan
- ExLibris security patches policy

- **Article last edited:** 17-March-2016