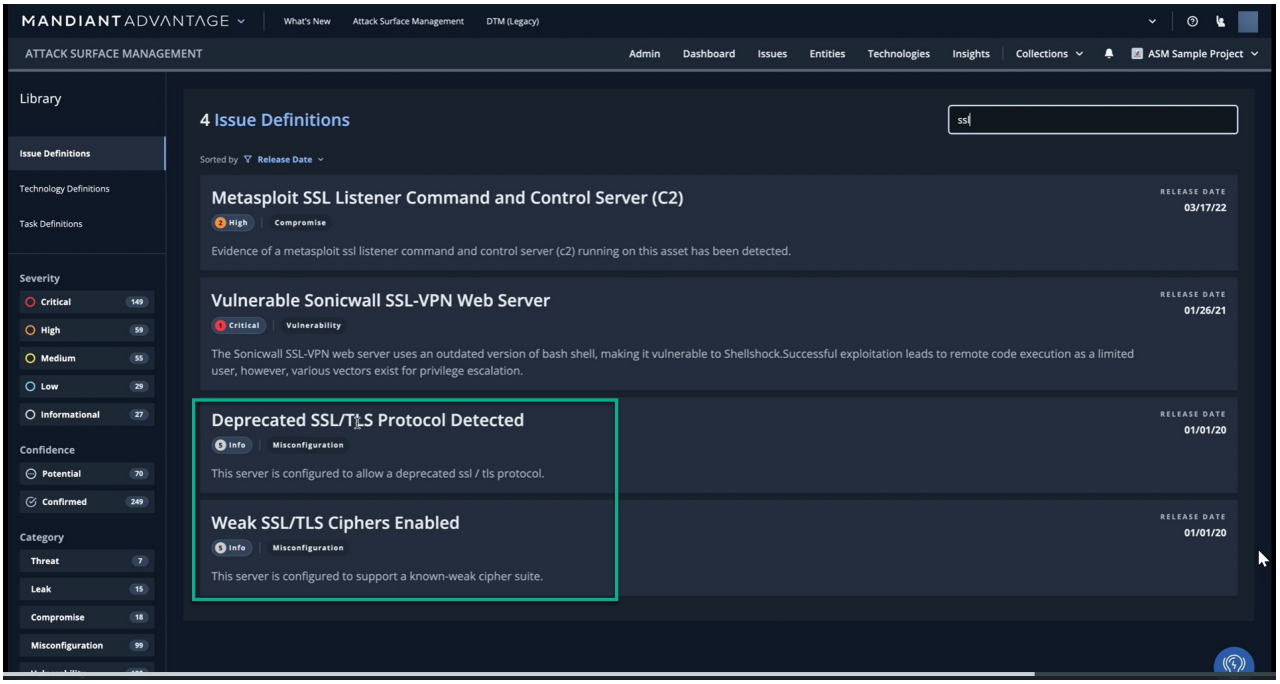
ANALYZING SSL/TLS ISSUES

For SSL/TLS vulnerability analysis in Mandiant Advantage Attack Surface Management (MA-ASM), two Issues are available:

- **Deprecated SSL/TLS Protocol Configured**: A vulnerability results when a server is configured to allow a deprecated SSL/TLS protocol.
- **Weak SSL/TLS Ciphers Enabled**: A vulnerability results when a server is configured to support a SSL/TLS cipher with a known low-sequence of encryption.

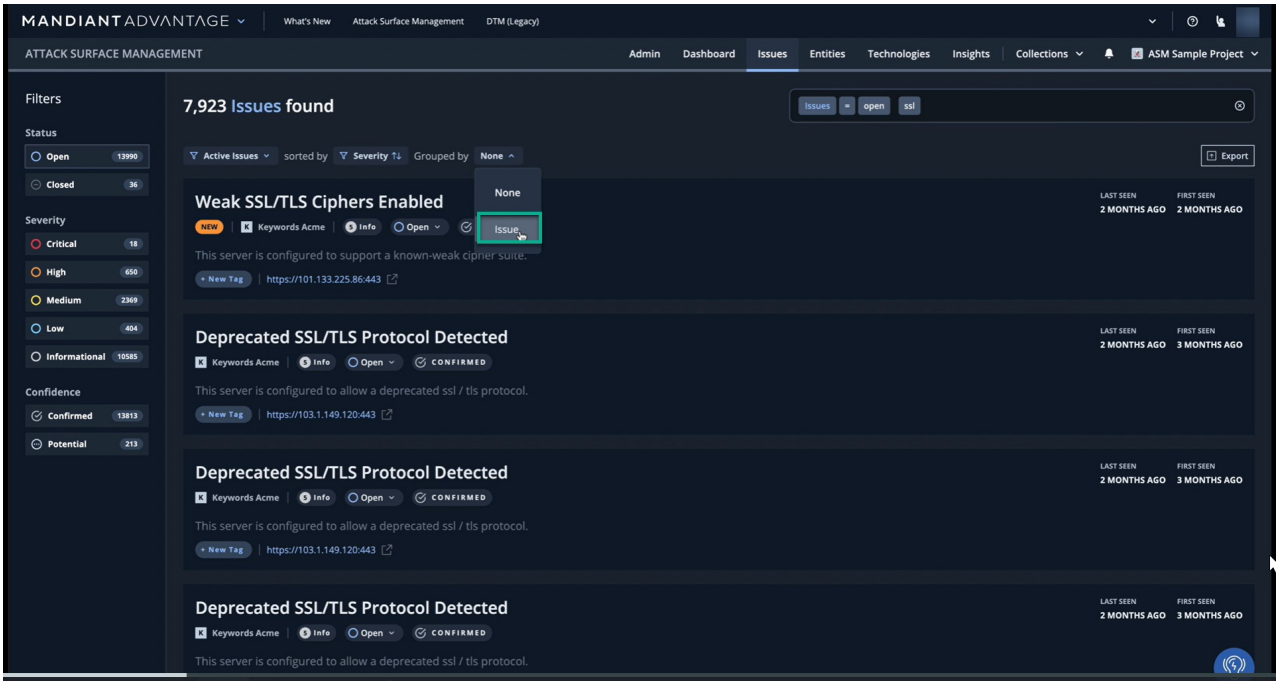
SSL/TLS Vulnerabilities in the Issue Definition Library

These Issues are defined in the Issue Definition Library. To locate both definitions, go to **Projects and Settings** > **Library**. From there, select **Issue Definitions** **(https://asm.advantage.mandiant.com/explorer/issues)**. Once the page comes up, enter **SSL** in the **Search for issues** bar.

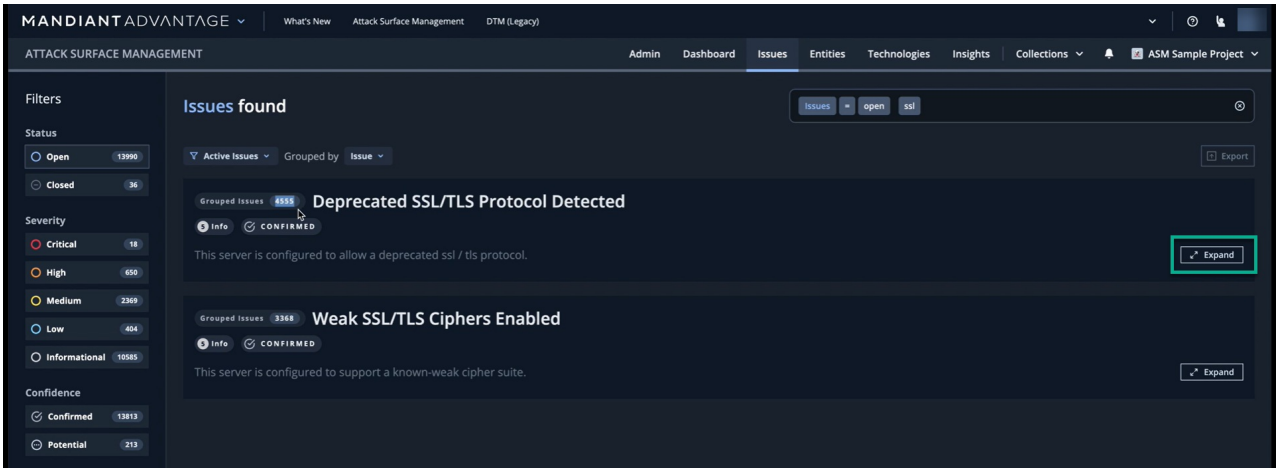


Access SSL/TLS Issues

To access specific Issues classified under either of these Issue Definitions, select the **Issues** tab in MA-ASM. Add **SSL** to the search bar and click **Enter**. Select **Issue** from the **Grouped by** drop down to cluster all SSL/TLS vulnerabilities that are present.



Click the **Expand** button to view a list of individual issues within each category.

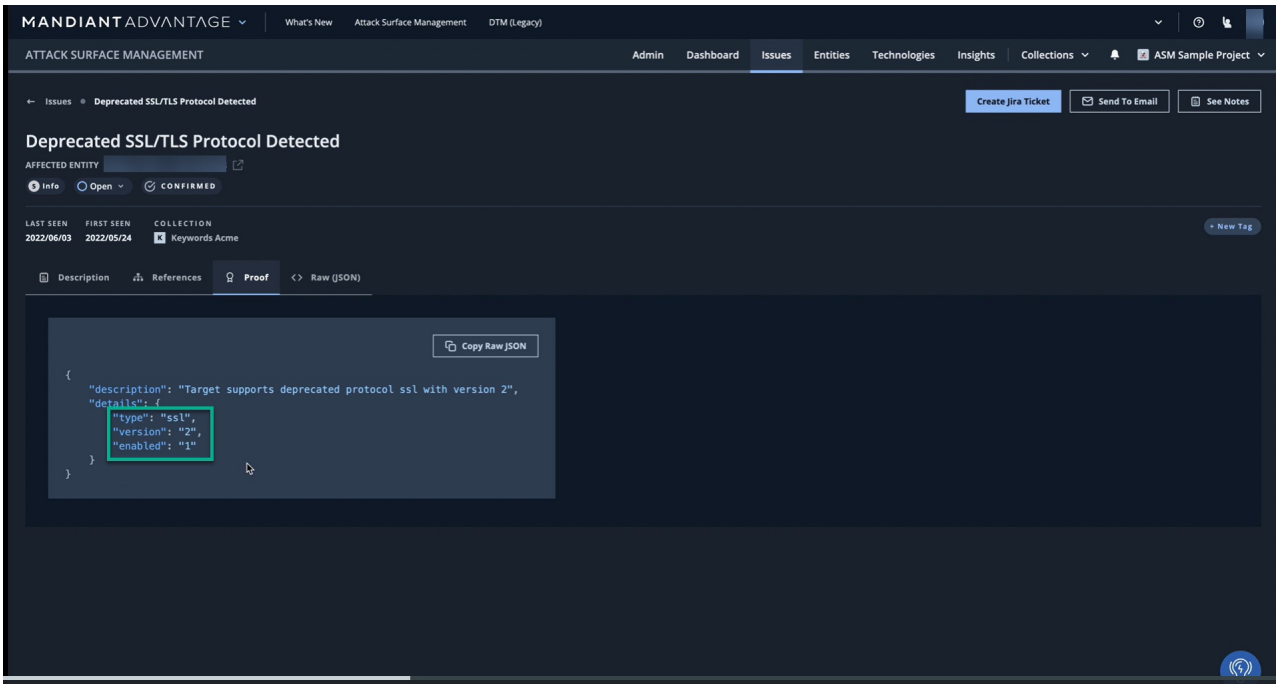


Choose one of the URLs from this list to explore more detailed **Description**, **References**, **Proof**, and **Raw (JSON)** information.

Examples

Example 1

In this example, the **Proof** for a **Deprecated SSL/TLS Protocol Detected** Issue shows that `version 2` of SSL protocol is enabled in the source.



Example 2

In this example, the **Proof** for a **Weak SSL/TLS Ciphers Enabled** Issue shows that known-weak SSL/TLS ciphers, `SHA256` & `SHA384`, are present in the source.