

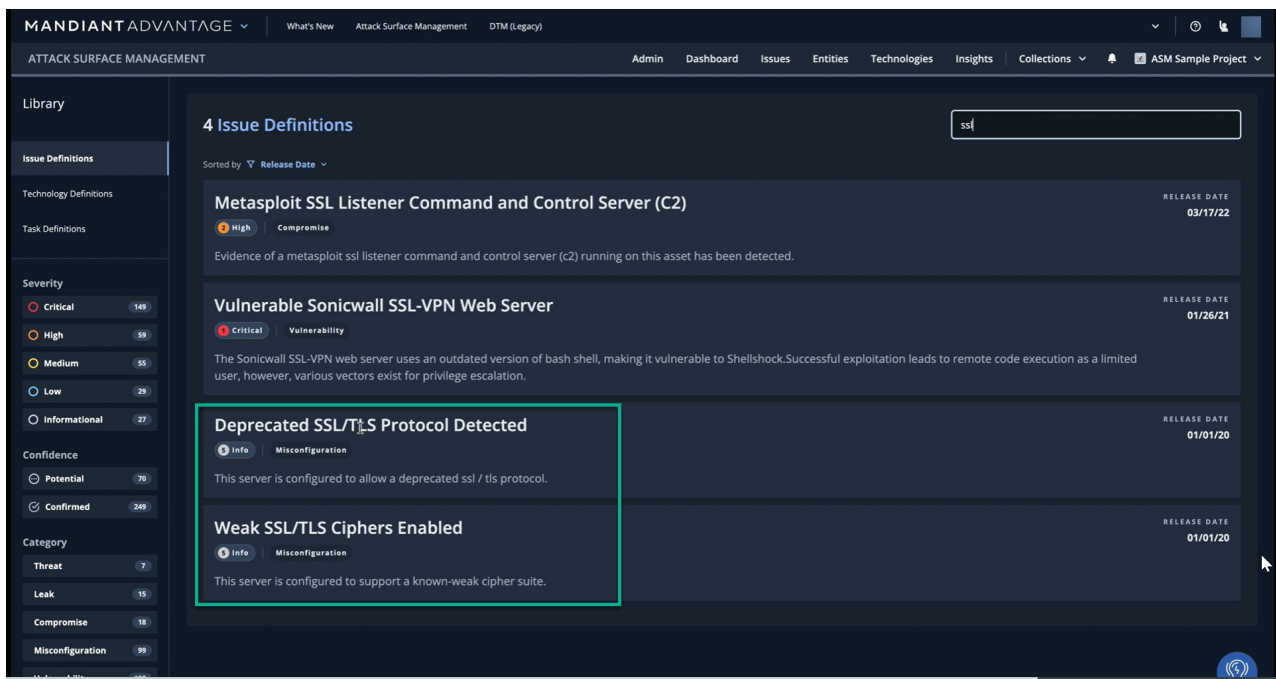
ANALYZING SSL/TLS ISSUES

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.

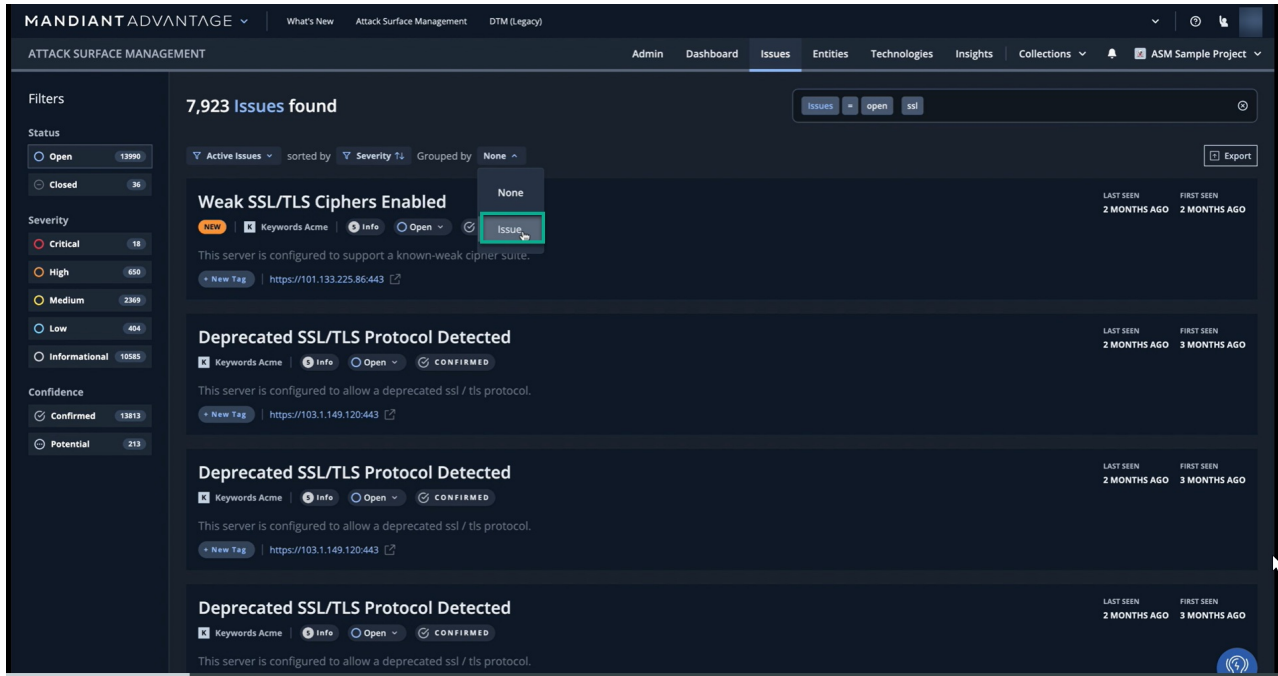


The screenshot displays the Mandiant Advantage Attack Surface Management (MA-ASM) interface. The top navigation bar includes 'MANDIANT ADVANTAGE', 'What's New', 'Attack Surface Management', and 'DTM (Legacy)'. The main navigation menu shows 'Admin', 'Dashboard', 'Issues', 'Entities', 'Technologies', 'Insights', 'Collections', and 'ASM Sample Project'. The left sidebar contains a 'Library' section with filters for 'Issue Definitions', 'Technology Definitions', 'Task Definitions', 'Severity' (Critical: 149, High: 59, Medium: 55, Low: 29, Informational: 27), 'Confidence' (Potential: 76, Confirmed: 249), and 'Category' (Threat: 7, Leak: 15, Compromise: 18, Misconfiguration: 99). The main content area shows '4 Issue Definitions' with a search bar containing 'ssl'. The issues listed are:

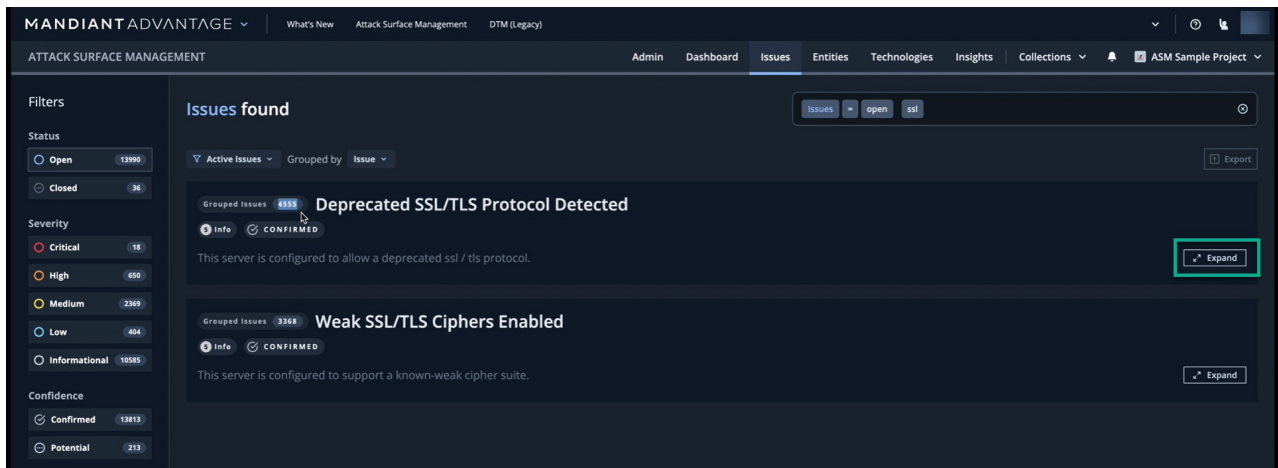
- Metasploit SSL Listener Command and Control Server (C2)** (High, Compromise, Release Date: 03/17/22)
- Vulnerable Sonicwall SSL-VPN Web Server** (Critical, Vulnerability, Release Date: 01/26/21)
- Deprecated SSL/TLS Protocol Detected** (Info, Misconfiguration, Release Date: 01/01/20)
- Weak SSL/TLS Ciphers Enabled** (Info, Misconfiguration, Release Date: 01/01/20)

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.

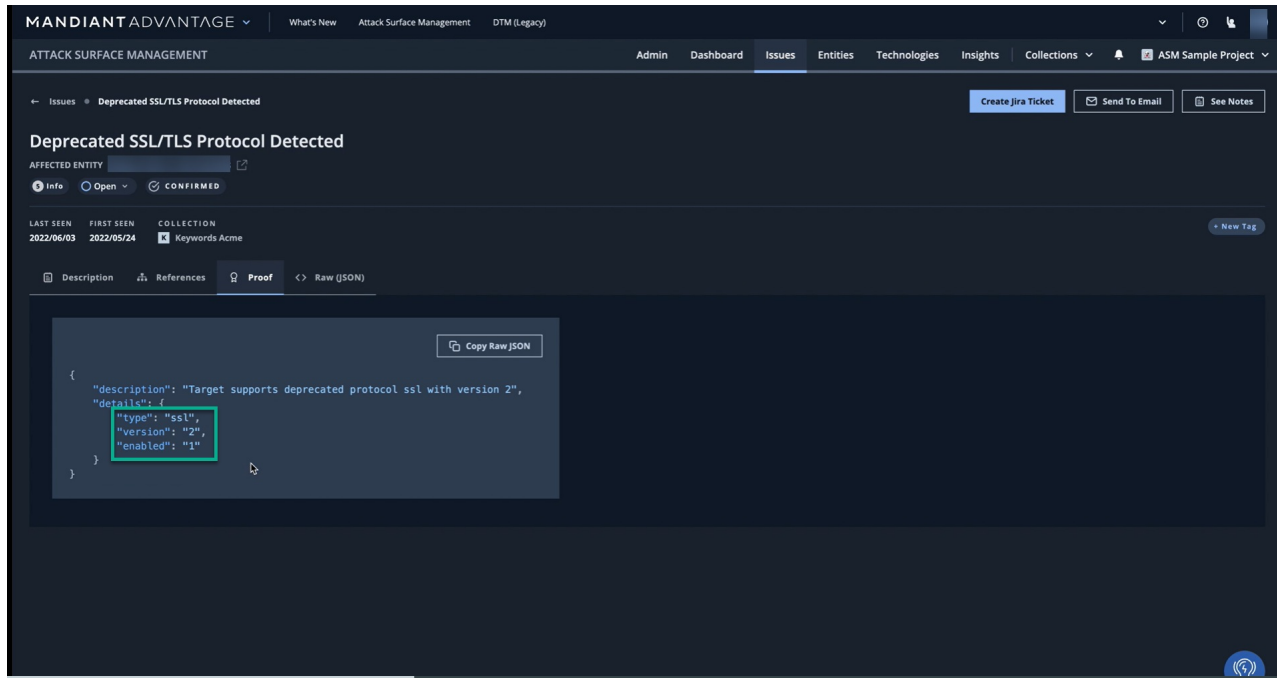


Choose one of the URLs from this list to explore more detailed **Description, References, Proof, and Raw (JSON)** information.

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.

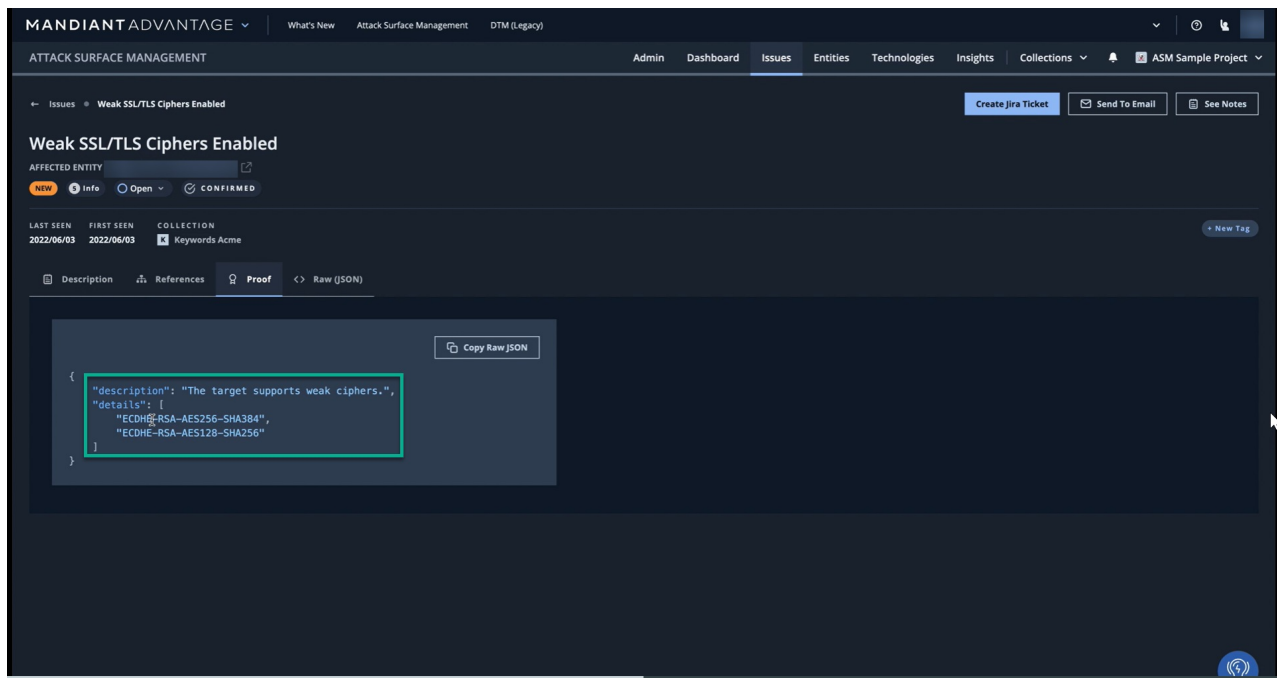


The screenshot displays the Mandiant Advantage interface for an issue titled "Deprecated SSL/TLS Protocol Detected". The interface includes a navigation bar with "ATTACK SURFACE MANAGEMENT" and "ASM Sample Project". The issue details show it is "CONFIRMED" and was first seen on 2022/05/24. The "Proof" tab is active, showing a JSON snippet with a red box highlighting the "type": "ssl", "version": "2", and "enabled": "1" fields.

```
{
  "description": "Target supports deprecated protocol ssl with version 2",
  "details": {
    "type": "ssl",
    "version": "2",
    "enabled": "1"
  }
}
```

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.



The screenshot displays the Mandiant Advantage interface for an issue titled "Weak SSL/TLS Ciphers Enabled". The interface includes a navigation bar with "ATTACK SURFACE MANAGEMENT" and "ASM Sample Project". The issue details show it is "NEW" and was first seen on 2022/06/03. The "Proof" tab is active, showing a JSON snippet with a red box highlighting the "ECDHE-RSA-AES256-SHA384" and "ECDHE-RSA-AES128-SHA256" fields.

```
{
  "description": "The target supports weak ciphers.",
  "details": [
    "ECDHE-RSA-AES256-SHA384",
    "ECDHE-RSA-AES128-SHA256"
  ]
}
```