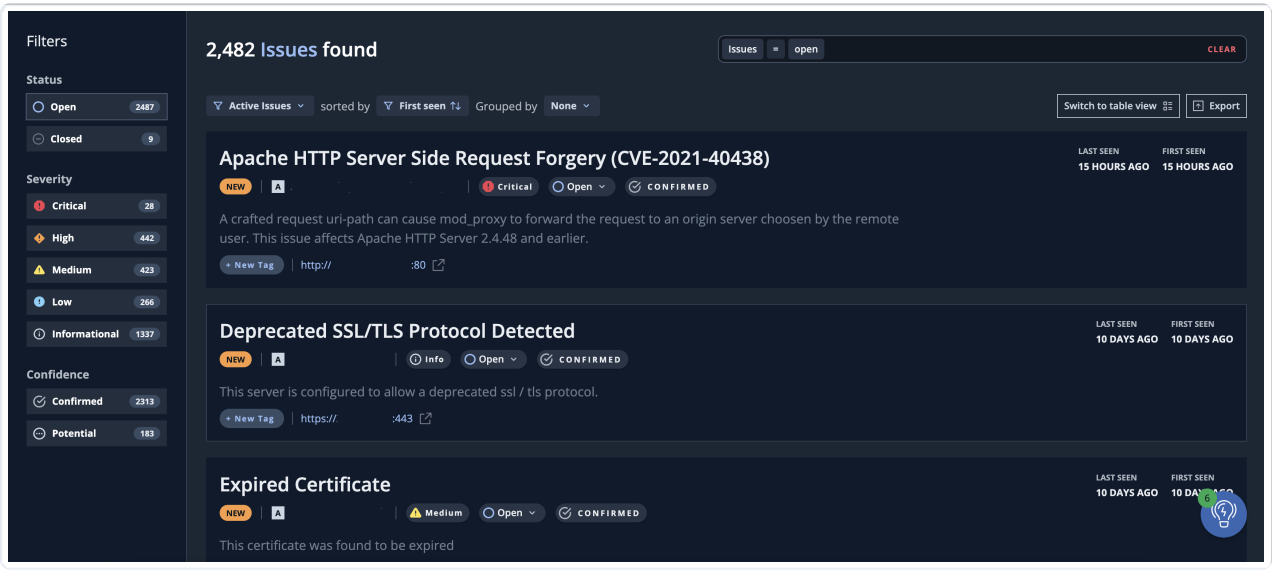
REVIEWING ISSUES

Issues are respective to the entity type, and different entity types warrant their own issue checks. The most common issue checks are for URI entities. Issue checks are selected based on the technology and version (as captured) that is fingerprinted on the Entity. So for example, a WordPress check will only run against an Entity that is fingerprinted with WordPress. This helps Mandiant Advantage Attack Surface Management (MA-ASM) to be more efficient and economical with resources, speeding up the scan and data gathering process.

Recent Issues List

The **Issues** page of MA-ASM shows you a list of the most recent Issues that were identified in the selected Collections. Each Issue listing contains:

- A short description of what was found
- The Collection containing the Issue
- Its **Severity** (https://docs.mandiant.com/home/asm-issue-severity-definitions-and-examples), **Status**, and **Confidence Level**
- Any tags associated with it
- The first and last times it was seen



Confidence Level

MA-ASM uses a **Confidence level** (https://docs.mandiant.com/home/asm-issue-severity-definitions-and-examples) of **Confirmed** or **Potential** to describe the degree of certainty that the Entity is actually vulnerable with the detected Issue.

- **Confirmed**: MA-ASM interacted directly with the target Entity to confirm that it was vulnerable with the associated Issue.
- **Potential**: Some form of inference was used to identify the Entity as being potentially vulnerable with the associated Issue.

Confidence level is driven by the type of check (active or passive) used to query the Entity in the Issues list:

- **Active Checks**: Most checks are active, which means MA-ASM sends a benign check directly to the target Entity to verify that it is indeed vulnerable. These payloads are strategically crafted to avoid any business disruptions to customer systems. Benign checks ensure that the integrity and availability of your systems are not compromised.

- **Passive Checks**: In scenarios where a public exploit cannot be verified without more aggressive methods, we passively determine that the system is potentially vulnerable based on the technology version.

For more information on checks, see **How Issues Work** (https://docs.mandiant.com/home/asm-how-issues-work).

Active and Inactive Filter

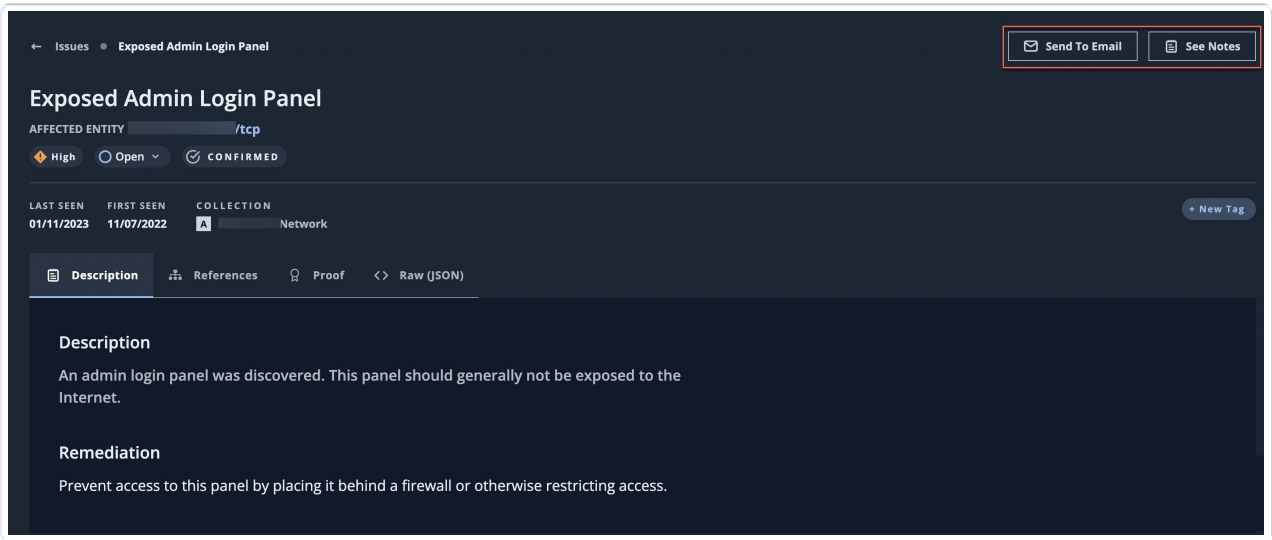
On the **Issues** page, you will see filter options including **Active Issues** and **Inactive Issues**:

- **Active Issues**: Issues that have been seen in the most recent scan.
- **Inactive Issues**: Issues that were seen in a previous scan and were not seen in the most recent scan.

Reviewing Issue Details

Clicking on an Issue allows you to send Issue details to an email address, review or add Notes, and drill down into additional components of the Issue:

- **Description**: Provides a short **Description** of the Issue and recommended **Remediation** steps, if available.
- **References**: Includes links to additional resources with greater details related to the detected vulnerability.
- **Proof**: Details the specific attributes of the query that triggered the successful detection of the vulnerability.
- **Raw (JSON)**: The raw JSON structure of the query itself.



Issue Status

A variety of status options are provided for tracking Issues. The following statuses are available under two categories, Open and Closed:

Open

Issues that are new or currently being worked.

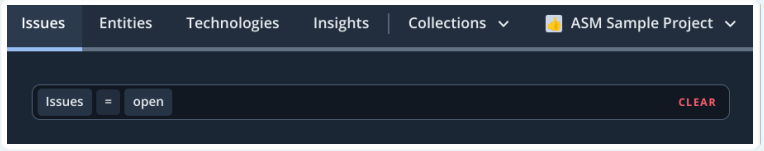
Status	Description
Triaged	The Issue is under review. You should validate the existence of the Issue within your operational environment.
In Progress	The Issue has been substantiated, and you are actively engaged in developing a resolution.

Closed

Issues that have been resolved and require no further action.

Status	Description
Mitigated	You have implemented an indirect resolution. The underlying issue persists but will be addressed by the foundational system.
Resolved	The Issue has been identified and successfully addressed.
Duplicate	The Issue is identical to an Issue that has previously been documented.
Out of Scope	The Issue falls outside of the defined scope.
Not a Security Issue (Benign)	The Issue has been reviewed and you have confirmed that it falls outside of your security guidelines.
Risk Accepted	You have confirmed the existence of the Issue but deemed it acceptable.
False Positive	This indicates an erroneous detection by the scan. The Issue should not have been reported.
Unable to Reproduce	You are unable to verify that the Issue exists as it is no longer available.
Tracked Externally	The Issue is being monitored and managed outside of MA-ASM.

- Only Issues with an Open status are included in **Custom Dashboard (https://docs.mandiant.com/home/ma-custom-dashboards)** widgets, unless otherwise specified.
- By default, when accessing the **Issues page (https://asm.advantage.mandiant.com/issues)**, the search parameters are set to only show Issues with an Open status.



Issues Library

A library of **Issue Definitions** is available from your **Projects and Settings > Library > Issue Definitions page (https://asm.advantage.mandiant.com/explorer/issues)** in MA-ASM. This comprehensive list shows the issue types we currently index, along with their **Severity** and **Confidence** ratings.