HOW ISSUES WORK

When inspecting an Entity for vulnerabilities, Mandiant Advantage Attack Surface Management (MA-ASM) performs one of the following types of probes:

- An *active* check, where a benign action is taken on the Entity to test for the existence of a known vulnerability
- *A passive* check, where the technology discovered on the Entity is used to infer potential vulnerabilities

The type of Entity determines the tasks used for probing, which in turn determines how the checks are performed. To learn more about each check, see the relevant section that follows:

- **Active checks**
- **Passive checks**

Active checks

If an active check is required, all payloads are strategically crafted to avoid any business disruptions to live environments. By using these benign actions, we ensure that we don't compromise the integrity and availability of the systems we are analyzing.

The following criteria are required for a vulnerability active check to be created and released:

- Detection of the vulnerability must be possible in unauthenticated form.
- The target must be reachable from the internet.
- A public exploit must exist.
- The vulnerability detection procedure must not damage or impact the target system in any significant way.

The following factors contribute to the prioritization of each vulnerability active check:

- Availability in Mandiant Advantage Threat Intelligence (MATI)
- CISA's Known Exploited Vulnerability list
- Internet-wise impact (particularly if remotely accessible without authorization)
- Is actively exploited or is known to be imminently exploited
- Customer request

Passive checks

In situations where a public exploit cannot be verified without more aggressive methods, MA-ASM performs a passive check to identify the technology (software and version) on the Entity. This information is then compared against our database of technologies that are known to be vulnerable. If a match is found in the database, then MA-ASM infers that a vulnerability could exist and raises an Issue about it. This type of passive check is often referred to as an *inference*.

However, some items like JavaScript libraries are vulnerable only when used in specific ways, so using just the inference method could potentially produce many false positives. In these cases, an augmented type of passive check is performed by MA-ASM, using additional heuristics to identify potential vulnerabilities. Again, no active checks are made, so anything identified is marked as a potential, not confirmed, vulnerability.

An example of how this comes into play is with the Log4j vulnerabilities.

Log4j

Log4j, originally developed by the Apache Software Foundation, is an open source library used for logging that is used by many different applications worldwide, including web services. Because it's incorporated into other applications and web

technologies, there are no actual markers or other external signs that Log4j is in use on any given site. This means that MA-ASM cannot perform a standard passive check to infer if any vulnerabilities exist on the web application directly because of it. Instead, MA-ASM sends a Log4j detection payload to every web application it encounters, and flags any interactions that are detected.

This detection method would be used for any other library or underlying system used to power an application. Because they are not web technologies themselves, there is no way for MA-ASM to determine with absolute certainty when they are actually in use. However, there are heuristics that can make a very educated assumption based on what other technologies are found – for example, if a website employs Java, then there's a strong likelihood that Log4j is being used. And based on that assumption, MA-ASM performs various other checks, including active checks specifically crafted to identify any exploitable configurations, to determine whether a potential vulnerability exists.

Issue Creation

Checks, both active and passive, yield Issues in MA-ASM, when vulnerabilities are detected or inferred:

- Issues detected by active checks are labeled with a **Confidence Level** **(https://docs.mandiant.com/home/asm-issue-severity-definitions-and-examples)** of Confirmed.
- Issues detected by passive checks are labeled with a Confidence Level of Potential.

For more information about Issues, see **Reviewing Issues** **(https://docs.mandiant.com/home/asm-issues)** and **ASM Issue Severity Definitions and Examples** **(https://docs.mandiant.com/home/asm-issue-severity-definitions-and-examples)**.

To familiarize yourself with the checks currently available in MA-ASM, see the **Task Library** **(https://docs.mandiant.com/home/asm-task-library)** documentation.