Mandiant

# ASM ISSUE SEVERITY DEFINITIONS AND EXAMPLES

This document describes how Mandiant Advantage Attack Surface Management (MA-ASM) determines the severity ratings for Issues.

## Confidence Level of Issues

MA-ASM uses triage categories to determine whether an Issue needs further investigation or is ready for review.

- **Confirmed**: MA-ASM has high confidence in the finding.
- **Potential**: There is a known vulnerability related to this Entity, but MA-ASM cannot confirm that this is true in this case.

Mandiant recommends prioritizing Confirmed Issues.

## Prioritization of Issues

Mandiant recommends giving priority to the resolution of **critical** and **high** severity Issues in order to strengthen the Entities associated with these Issues. As a customer, you iterate on the MA-ASM program. You and other team members discuss how you can effectively triage **medium** and **low** severity Issues over time. Discussions could be about a ticketing system or whether channels of communication are open to infrastructure or technology owners.

The following table, Issue Severity Definitions, outlines a common understanding of the risks of vulnerability, misconfiguration, and exposure.

| Issue Severity Definitions | | |
|---|---|---|
| **Issue Severity** | **Definitions** | **Examples** |
| Critical | The asset has an increased risk of exploitation based on activity observed in the wild, or the potential exposure and data leakage will negatively affect the organization. Successful exploitation could allow a threat actor to achieve persistence, lateral movement, account compromise, or data exfiltration. A CVE **CVSS (https://nvd.nist.gov/vuln-metrics/cvss)** 9.0-10.0 and a Critical Risk Rating from Mandiant validate the issue severity.<br>Suggested Usage:<br>• Investigate within 24 hours<br>• Remediate within 7 days | • Gitlab - Account Takeover via SCIM (**CVE-2022-1680 (https://nvd.nist.gov/vuln/detail/cve-2022-1680)**)<br>• Atlassian Confluence Server - Arbitrary Code Execution (**CVE-2022-26134 (https://nvd.nist.gov/vuln/detail/cve-2022-26134)**)<br>• vBulletin Unauthenticated Remote Code Execution (**CVE-2019-16759 (https://nvd.nist.gov/vuln/detail/cve-2019-16759)**)<br>• Log4j aka Log4Shell Unauthenticated Remote Code Execution (**CVE-2021-44228 (https://nvd.nist.gov/vuln/detail/cve-2021-44228)**) |

| Issue Severity Definitions | | |
|---|---|---|
| High | The asset has a vulnerability, misconfiguration, or exposure that, when exploited or leveraged by a threat actor, can enable them to achieve persistence or lateral movement or perform unauthenticated actions. CVEs with a **CVSS (https://nvd.nist.gov/vuln-metrics/cvss)** of 7.0-8.9 or a High Risk Rating from Mandiant Threat Intelligence generate high severity Issues.<br>Suggested Usage:<br>• Investigate within 48 hours<br>• Remediate within 14 days | • Exposed RDP or SMB<br>• **Command and Control (C2) Server (https://csrc.nist.gov/glossary/term/command_and_control)** Identified<br>• World Writeable AWS S3 Bucket |
| Medium | The asset is vulnerable; however, the affect of exploitation is offset by hardening methods such as MFA or additional access requirements that hinder a threat actor from achieving their mission.<br>Suggested Usage:<br>• Investigate within 72 hours<br>• Remediate within 21 days | • Exposed VPN Service<br>• Exposed Databases<br>• A 2FA which can be bypassed |
| Low | The asset has a vulnerability, misconfiguration, or exposure that can further a threat actor's reconnaissance effort, but does not pose an immediate risk.<br>In some organizations, low severity Issues are considered acceptable.<br>Suggested Usage:<br>• Investigate within 4 days<br>• Remediate within 28 days | • World Readable AWS S3 Buckets<br>• Wildcard Certificates<br>• Security Headers Missing from URL |
| Informational | Security hygiene insights that do not require immediate attention but should be addressed during ongoing efforts to improve security posture. You may choose to delegate informational Issues to the appropriate team.<br>Suggested Usage:<br>• Investigate within 1 month<br>• Remediate within 3 months | • Self-signed Certificates<br>• Deprecated SSL/TLS Protocols<br>• Insecure Cookies |

### Numeric Severity

A numeric severity system is used when configuring some **MA-ASM outbound integrations (https://docs.mandiant.com/home/asm-outbound-integrations)**. The following table outlines the numbers associated with each Issue Severity level in MA-ASM.

| Numeric Severity for Issues | |
|---|---|
| **Issue Severity** | **Numeric representation** |
| Critical | 1 |
| High | 2 |
| Medium | 3 |
| Low | 4 |
| Informational | 5 |