Troubleshoot FMC Intrusion Events Showing Impact=Unknown

Contents

Issue

After deploying a new Firewall Management Center (FMC) and upgrading to version 7.7.12, all intrusion events are displaying "Impact=Unknown" instead of the expected impact values. This prevents proper alerting mechanisms from triggering, as the impact field is required for alert configuration.

Environment

- FMC version 7.7.12. Other software versions can be also affected.
- Intrusion Policy in Prevention or Detection mode.

Resolution

The resolution for this issue involves verifying and configuring the discovery policy scope to include all relevant IP addresses where intrusion events are generated.

Step 1. Identify Affected IP Addresses

Review the intrusion events that are showing "Impact=Unknown" and identify the specific IP addresses involved in these events. Document these IP addresses for comparison with the current discovery policy configuration.

Step 2. Review Current Discovery Policy Configuration

Navigate to the FMC **Policies > Network Discovery** (in newer versions is **Policies > Advanced > Network Discovery**) and examine the current discovery policy settings to determine which IP address ranges or subnets are currently included in the discovery scope.

Step 3. Update Discovery Policy Scope

Modify the discovery policy configuration to include all IP addresses where intrusion events are occurring. Ensure that the discovery policy scope encompasses all network segments where you expect to receive intrusion events with proper impact assessment.

Step 4. Deploy Configuration Changes

Deploy the updated discovery policy configuration to all managed devices to ensure the changes take effect across the entire security infrastructure.

Step 5. Verify Impact Field Population

Monitor new intrusion events to confirm that the impact field is now being populated with appropriate values instead of "Unknown".

Cause

The intrusion events showing "Impact=Unknown" were caused by a configuration issue where the affected IP addresses were not included in any discovery policy on the FMC. When IP addresses fall outside the scope of configured discovery policies, the FMC cannot properly assess the impact of intrusion events for those addresses, resulting in the impact field being populated with "Unknown" values. This is a configuration-related issue rather than a software or hardware defect.

Related Content

- Intrusion Event Impact Levels
- Cisco Technical Support & Downloads