对显示Impact=Unknown的FMC入侵事件进行故障排除

目录

问题

部署新的防火墙管理中心(FMC)并升级到7.7.12版后，所有入侵事件显示“Impact=Unknown”，而不是预期影响值。这会阻止触发适当的警报机制，因为警报配置需要影响字段。

环境

- FMC版本7.7.12。其它软件版本也可能会受到影响。
- 入侵策略(Intrusion Policy)在防御或检测模式。

分辨率

此问题的解决涉及验证和配置发现策略范围，以包括生成入侵事件的所有相关IP地址。

步骤1.确定受影响的IP地址

查看显示“Impact=Unknown”的入侵事件并确定这些事件中涉及的特定IP地址。记录这些IP地址，以便与当前发现策略配置进行比较。

步骤2.查看当前发现策略配置

导航到FMC Policies > Network Discovery(在较新的版本中，为Policies > Advanced > Network Discovery)，检查当前的发现策略设置，以确定当前发现范围内包含的IP地址范围或子网。

步骤3.更新发现策略范围

修改发现策略配置，使其包含发生入侵事件的所有IP地址。确保发现策略范围包含您预期接收入侵事件的所有网段，并进行适当的影响评估。

步骤4.部署配置更改

将更新的发现策略配置部署到所有受管设备，以确保更改在整个安全基础设施中生效。

步骤5.检验影响字段填充

监视新的入侵事件，以确认影响字段现在已填充适当的值而不是“未知”。

原因

显示“Impact=Unknown”的入侵事件是由配置问题引起的，其中受影响的IP地址未包括在FMC上的任何发现策略中。当IP地址不在已配置的发现策略范围内时，FMC无法正确评估入侵事件对这些地址的影响，从而导致影响字段填充了“未知”值。这是与配置相关的问题，而不是软件或硬件缺陷。

相关内容

- 入侵事件影响级别
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。