验证VDB直接更新路径和流量对FMC的影响

目录

问题

当在漏洞数据库(VDB)更新上运行时，管理员需要了解VDB更新是否为累积更新，以及是否可以跳过中间版本。

在本示例中，问题是从VDB版本393更新到版本427时需要考虑的问题。具体来说，不确定是否需要多个升级步骤或是否支持直接升级路径。此外，还担心VDB更新和后续策略部署过程中可能出现的服务中断。

环境

- 安全防火墙管理中心(FMC)软件版本7.4.2.4。其他软件版本也受到影响。
- FPR 2110上的防火墙威胁防御(FTD)。其他硬件平台也受到影响。
- 当前VDB版本：393.其他软件版本也受到影响。
- 目标VDB版本：427.其他软件版本也受到影响。

分辨率

FMC上的VDB更新是累积性的，允许从旧版本直接升级到新版本，无需中间步骤。

VDB更新过程

您可以直接从VDB版本393更新到VDB版本427，无需任何中间VDB升级步骤。从VDB版本357开始，思科支持在FMC平台上安装任何早于基准VDB的VDB版本。

要下载最新的VDB版本，请参阅软件下载。

服务影响注意事项

主要风险不与FMC上的VDB安装本身相关联，而是与VDB更新后FTD上的第一个策略部署相关联。在大多数情况下，VDB更新后的第一个部署会重新启动Snort进程，这会暂时中断流量检查。

在此中断期间：

- 流量可以丢弃或通过，无需进一步检查。
- 具体行为取决于FTD如何配置为在进程重新启动期间处理流量。

最佳实践建议：

- 在计划的维护时段内安排策略部署部分。
- 与网络运营协调以最大程度降低对用户的影响。
- 在部署过程中和部署之后监控系统状态。

原因

- 从VDB 357开始，您可以安装任何早于FMC基准VDB的VDB更新。
- 安装需要重新部署策略以激活新的漏洞签名，这会触发受管FTD设备上的Snort进程重新启动。此重新启动会在加载新数据库并重新初始化检测引擎时短暂中断流量检测功能。

相关内容

- Cisco Secure Firewall Management Center管理指南 — 系统更新

- 思科安全防火墙管理中心设备配置指南 — 部署
- 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）。