安全访问基于客户端的ZTA状态配置和行为规范

目录

问题

当用于互联网访问时，出现了有关思科安全访问基于客户端的零信任访问(ZTA)终端安全评估功能的特定行为和配置功能的问题。具体关注问题包括：

- 操作系统状态要求是否支持可配置的宽限期（最多365天），在此期间，设备仍可使用ZTA模块访问互联网目标，即使它们不符合所需的操作系统版本。
- 除操作系统以外的安全评估要求（如防火墙、系统密码等）是否会在未满足时立即阻止目标访问。
- 是否可以通过安全访问GUI界面为安全状态要求故障配置自定义警告消息或阻止以外的操作（如监控）。

环境

- 具有零信任访问(ZTNA)功能的思科安全访问
- 基于客户端的ZTA状态实施
- 互联网接入使用案例场景
- 安全评估要求，包括操作系统、防火墙和系统密码条件

分辨率

下面几节中介绍的有关安全访问基于客户端的ZTA终端安全评估行为和配置功能的说明。

操作系统状况宽限期

描述的操作系统状态要求行为是正确的。配置操作系统安全评估条件后，它支持可配置的宽限期（最多365天）。在此宽限期内，不满足所需操作系统版本的设备在升级到目标版本时，仍然可以使用ZTA模块访问互联网目标。

非操作系统状态要求

对于操作系统以外的安全评估条件（例如防火墙、系统密码和其他安全控制），当这些要求未得到满足时，会立即阻止对目标的访问。这些状态类型不支持可用于操作系统要求的宽限期功能。

安全评估故障操作和自定义消息

状态要求失败的操作通过访问策略配置控制。

访问策略支持多种操作类型，包括：

- 允许
- 阻止
- 警告
- 隔离

安全评估失败的自定义警告消息和通知页面可以通过访问策略安全配置文件设置配置。通过Manage Notification Pages文档和配置界面处理警告和通知页面管理。

这意味着除阻止之外的其他操作（如通过“警告”操作进行监控）是可用的，并且可以进行配置，这与只可能阻止操作的初始评估相反。

原因

这些问题源于需要了解操作系统状态要求和其他状态类型之间的具体行为差异，以及澄清安全访问GUI界面中无法立即显现的状态故障处理的可用配置选项。

相关内容

- 管理安全访问的通知页面文档
- 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）。