Google Drive安全下载期间发生CRYPTO_INTERNAL_ERROR

目录

问题

通过启用了流量解密的思科安全访问访问加密的Google Sheets文件时无法打开。用户在Google Drive安全下载期间会遇到CRYPTO_INTERNAL_ERROR。当安全Web网关(SWG)检测处于活动状态时，会特别出现此问题，因为在解密和检测过程中忽略Range报头，导致对Google安全下载机制的干扰。

此问题会影响使用RAVPN+ZTA实施的环境，并影响对大量用户访问加密的Google Sheets。

环境

- 技术：思科安全访问（解决方案支持）
- 子技术：安全访问
- 实现：RAVPN+ZTA（远程接入VPN +零信任接入）
- 受影响的组件：ZTA配置文件
- 受影响的域：clients6.google.com和其他Google Drive相关的域

分辨率

解决方案涉及实施临时解决方法，同时监控永久供应商端修复。

以下各节概述的方法已经过验证，可以恢复对加密的Google表格的访问。

临时解决方法选项

选项 1：禁用流量解密

完全禁用受影响用户组或策略的流量解密。这将恢复Google Sheets访问，但会删除所有基于解密的安全检查功能。

选项 2：从解密中排除Google驱动器域

将Google驱动器相关的域添加到安全访问策略配置中的不解密列表：

- clients6.google.com
- 流量分析中确定的其他与Google Drive相关的域

此方法可以维护其他流量的解密，同时允许Google Sheets正常工作。但是，此解决方法可以权衡禁用排除域的CASB Google Drive上传阻止功能。

技术分析和监控

思科分析确认，安全网关检测会忽略范围报头，以实现文件内容的全面安全扫描。此行为会干扰Google Drive安全下载过程，该过程依赖于Range标头来实现正确的解密流程。

Google已承认此问题，并确定代理行为（包括Cisco Umbrella/网络代理）通过删除或重写Range标头来干扰Google Drive安全下载请求。这会强制下载完整文件，从而破坏Google解密机制。Google正在开发客户端解决方案，不过尚未提供预计到达时间。

实施注意事项

实施解决方案的组织应考虑安全影响：

- 评估从解密检查中排除Google Drive域的风险。
- 查看可能受域排除影响的CASB策略。
- 记录将来政策审查的临时解决方法。
- 监控Google有关客户端修复开发的最新信息。

原因

根本原因是思科安全访问SWG检查行为和Google Drive安全下载机制之间的兼容性问题。

具体来说：

在解密和安全扫描过程中，Cisco安全Web网关检测会忽略Range报头，以确保完整的文件分析。但是，Google Drive加密文件访问依赖于Range标头来正确处理安全下载的解密流程。在代理检查过程中删除或修改这些报头时，Google客户端解密失败，导致CRYPTO_INTERNAL_ERROR。

这表明安全检查要求（完整文件扫描）和Google加密文件传输机制（基于范围的安全下载）之间的根本不兼容。

相关内容

- 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）。