

没有数据分类的安全访问DLP文件大小规则不会生成文本文件的监控事件

目录

问题

仅使用文件大小条件（无数据分类）配置的思科安全访问Web DLP策略不会为.txt文件上传生成DLP监控事件，而同一策略会其他文件类型（如.xlsx、.png和.pdf文件）正确触发监控事件。受影响的策略Advanced Management Policy - Web配置有：

- 自定义文件大小在1KB和49MB之间的文件控制
- 无数据分类标准
- 设置为监控的操作

测试显示：

- Action = Monitor时，TXT文件上传不会显示在DLP事件中。
- 当Action = Block时，相同的TXT文件会正确生成DLP事件。
- 活动日志显示所有文件上传，包括TXT文件。
- 其他文件格式(PNG、PDF、XLSX)会使用“监控”(Monitor)操作按预期生成DLP事件。

此外，在DLP规则中未配置数据分类时，无论配置的规则严重性设置如何，记录的DLP事件始终显示Medium严重性。

环境

- 思科安全访问（以前称为Cisco Umbrella）
- DLP（防数据丢失）Web策略

- 启用HTTPS解密的互联网访问策略
- 通过Web应用程序执行文件上传测试

分辨率

此行为没有记录，但设计上是预期的。当使用仅文件大小条件和“监控”(Monitor)操作来防止日志过载时，会从DLP监控中绕过文本/纯文本等MIME类型。开发团队证实，这是没有外部记录的故意行为。

解决方法选项

选项1 (推荐) : 添加数据分类

在DLP规则中添加任何广泛的数据分类条件，同时保留Action = Monitor。

这将恢复：

- TXT文件DLP事件生成
- 根据规则配置更正严重性处理

选项 2 : 将操作更改为阻止

将规则操作从Monitor更改为Block。这会为TXT文件生成DLP事件，但也会强制阻止仅监控使用案例不需要的内容。

实验室测试结果

全面的实验室测试证实了行为模式。

测试场景1:具有数据分类和文件大小的DLP规则(1KB-49MB)，操作=阻止

- TXT文件与PII:已阻止和已记录
- PDF文件：已阻止和已记录
- 不带PII的TXT文件：允许（预期）
- 使用PII的PNG:允许（基于分类而预期）

测试场景2:仅具有文件大小的DLP规则（无数据分类），操作=阻止(Block)

- 所有文件类型(TXT、PDF、PNG):已阻止和已记录
- 尽管规则配置为低，严重性仍显示为中

测试场景3:仅具有文件大小的DLP规则（无数据分类），操作=监控

- TXT文件：允许但未登录DLP事件
- PDF和PNG文件：允许并登录DLP事件
- 活动日志显示所有上传，包括TXT文件

原因

这是思科安全访问DLP中的有意但未记录的行为。当使用仅文件大小规则和“监控”(Monitor)操作来防止生成过多的日志时，系统会绕过文本/纯文本MIME类型的DLP事件日志记录。行为取决于操作且特定于MIME类型：

- 使用仅文件大小条件监控操作：从日志中绕过的TXT文件

- 使用仅文件大小条件阻止操作：正常记录的TXT文件
- 存在数据分类的任何操作：正常记录的TXT文件

出现严重性问题的原因是，在内容感知模式下运行时，DLP事件从数据分类元数据而不是规则设置获取严重性。如果没有数据分类，无论配置的规则严重性如何，系统都会默认为“中”严重性。

相关内容

- [思科安全访问DLP文件大小配置](#)

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）。