思科安全终端覆盖请求最佳实践

目录

简介

本文档介绍为已识别但安全终端当前未检测到的已知威胁请求Talos覆盖时必须使用的流程。

不同的信息来源

可以有多个来源来识别和发布这些威胁，以下是一些常用的平台：

- 已发布Cisco CVE
- 已发布的CVE（常见漏洞和暴露）
- Microsoft建议
- 第三方威胁情报

在让Talos审核信息和确定相关覆盖范围之前，思科希望确保数据源是合法的。

为了审查思科对有关威胁的立场和覆盖范围，我们有各种思科/Talos资源，在请求新的覆盖范围请求之前，必须对这些资源进行审核。

思科漏洞门户

有关与思科产品相关的任何CVE，请查看此门户了解更多信息：https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Talos门户

Talos情报门户必须成为查看此威胁是否已调查或当前是否由Talos调查的第一个参考点：https://talosintelligence.com/

Talos博客

思科Talos博客还提供有关Talos评估和调查的威胁的信息：https://blog.talosintelligence.com/

我们能够找到“Vulnerability Information”（漏洞信息）下的大多数相关信息，其中还包括所有已发布的“Microsoft Advisories”（Microsoft建议）。

使用思科产品进行其他调查

思科提供多种产品，可帮助查看威胁媒介/散列，并确定安全终端是否提供威胁覆盖范围。

Cisco SecureX思科威胁响应调查(CTR)

我们可以在CTR调查中调查威胁载体，有关详细信息，请访问：https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html

Cisco XDR调查

Cisco XDR提供用于调查威胁载体的增强功能，有关功能的详细信息，请访问：https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm

有用的思科博客

请阅读这些博客，了解上一节讨论的一些功能：

https://blogs.cisco.com/tag/relevant-and-extended-detection-with-securex

后续步骤

如果我们找不到使用上述步骤涵盖的威胁载体，我们可以通过提交TAC支持请求来请求威胁的Talos覆盖范围。

https://www.cisco.com/c/en/us/support/index.html

为了加快覆盖请求的评估和调查，我们将请求以下有关威胁的信息：

- 威胁情报的来源(CVE/Advisory/第三方调查/技术说明/博客)
- 关联的SHA256散列
- 文件示例（如果可用）。

信息可用后，Talos将审核并相应地调查请求。

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）。