思科安全终端覆盖请求最佳实践

目录

简介

不同的信息来源

- 思科漏洞门户
- Talos门户
- Talos博客

使用思科产品进行其他调查

- Cisco XDR调查
- 有用的思科博客

后续步骤

概述

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：思科漏洞门户

Talos门户

Talos情报门户必须成为查看此威胁是否已调查或Talos当前是否正在调查的第一个参考点：Talos门户

Talos博客

Cisco Talos博客还提供有关Talos评估和调查的威胁的信息：Talos博客

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 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，请访问以下网址：Cisco XDR调查

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，如思科扩展检测和响应

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支持请求来请求该威胁的Talos覆盖。

为加快覆盖请求的评估和调查，我们将请求以下信息：

- 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）。



注意：对于与渗透测试或红色组合相关的覆盖请求，要求可能会因测试类型而异。在某些情况下，可能需要客户提供更多的信息。提供所需信息后，Talos将相应审核、评估和调查请求。

概述

收到所需信息后，我们开始一个专门的审核流程。为确保提供最高级别的保护，交付时间表受以下几个关键因素指导：

定制分析
由于每个威胁场景和客户环境都是独一无二的，因此我们执行自定义验证以确保有效的安全保护，而不会中断您的业务运营。

数据驱动的响应
相关遥感勘测、人工或恶意软件样本的可用性直接支持我们的分析速度。

严格的质量保证
为了保持产品的稳定性和可靠性，每个解决方案都要进行全面的测试和分阶段部署。

安全版本管理
我们将更新与既定的发布周期保持一致，以确保以可控且可靠的方式提供所有保护。

自适应保护
安全是一个持续的过程。部署后，我们会持续监控和调整检测，以领先于不断演变的威胁形势。

确定关键问题的优先级
我们逐个评估每个请求。通过加速的工作流程自动快速跟踪涉及高严重性漏洞、主动漏洞利用或严重误报的问题，从而最大限度地降低风险。

我们非常感谢您的合作，我们将努力提供强大、准确的保护，确保您的组织安全且高效。

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）。