2016 年 11 月 28 日 星期一

Talos 更新负责任的披露政策

负责任的漏洞披露是安全研究的一个重要方面。要做到负责任的披露，通常比较难的一点在于在相互冲突的利益之间取得平衡：一方面要协助供应商对产品打补丁，另一方面要通知大众预防零日漏洞。我们不得不承认的一点是如果白帽客团队发现了高价值目标存在的漏洞，那他们的对手也很可能正在尝试利用该漏洞。研究人员必须谨慎地在供应商的需求和功能之间取得平衡，以解决产品存在的问题，并将客户和社区的安全视为一个整体。

Talos 已对负责任披露政策相关的时间表、行业回应和最终结果进行了测量。今天，我们要宣布所做的一些改变。有关完整的《供应商漏洞报告和披露政策》，请访问以下网址：http://www.cisco.com/c/en/us/about/security-center/vendor-vulnerability-policy.html。

这些改变包括根据供应商反馈对时间表做出的调整，以及自上次谈到我们的《披露政策》以来行业内出现的变化。

时间表调整

今天，Talos 宣布对时间线政策做出调整，以确立 90 天的披露期。此项改变是基于以下因素做出的：供应商反馈、打补丁平均所需时间（我们的漏洞研究团队得出的数据）以及通过确保在适宜时间段内进行有效的漏洞披露以增强对日常互联网用户的保护。下面列出了已更新《披露政策》中的几个关键阶段。Talos 将在适当的时候与供应商一起审阅时间表目标，从而充分地提供打补丁所需的时间。审阅时会具体情况具体分析，以确保打补丁进度有所增长。如果出现情有可原的情况（例如：出现任何性质的威胁），则披露和时间表可能要提前或延后。

零日	· 初始供应商联系人 · 向使用思科安全产品的客户发布的保护工具
七日	· 未收到回应时的第二供应商联系人
十五日	· 在思科漏洞跟踪网站上发布供应商通知日期
四十五日	· 如果供应商未作出回应，漏洞报告将转发至 CERT。
九十日	· CERT 根据其协调原则公开发现的漏洞 · 当相关补丁或缓解措施发布之后或期限到期之后，在 Talos 漏洞跟踪网站上发布完整的漏洞公开报告

如果供应商在初次联系后的 45 天内都没有给予回应，则漏洞报告还将被递交至卡内基·梅隆大学的计算机应急小组 (CERT)。根据 CERT 漏洞披露指南的规定，供应商在漏洞信息被公开披露之前大约有 45 天的时间。

我们来看下我们在供应商时间表和打补丁时间 (TTP) 方面的发现。在所有供应商中，总体平均打补丁所需时间为 78 天。第一眼看去，商业供应商的速度似乎比开源供应商慢很多。但细分一番之后，我们发现了一些有趣的信息：

所有商业供应商 TTP		所有开源供应商 TTP	行业平均值
> 80 天		42 天	78 天
领先平均 TTP	落后平均 TTP		
113 天	38 天		

数据来源于 143 个 Talos 错误报告样本。

此处反映的细微差别较首行数据要多一些。具体来说，商业供应商分可划分为领先类（在策略时间范围内）和落后类（耗时超过既定时间范围）。值得关注的是，几个大型的消费者软件供应商都属于领先类。在我们的数据中，“快速周转商业”供应商表示回应最迅速的一些供应商 - 他们具备一些共同特征。他们都是大型的流行消费者软件供应商，都公开表明过在产品安全方面的态度，并且都正在实施错误赏金计划。可以看出，这些公司都对产品安全进

行了大量投资，并且十分重视安全性。在打补丁时间方面，他们可以比得上一些开源公司。令人振奋的是此类公司的数量正在不断增加，尽管商业供应商中落后天数最多的供应商将整体平均值从 40 天拉长至 78 天。据传，在此期间一个开源供应商创造了新的一天之内解决问题的“速度记录”。

行业发展

从我们的数据中可以看出一股向上的趋势。显然，供应商意识到零日漏洞可能给客户带来严重的经济影响。此外，丢失市场信誉可能对供应商及其客户都造成无法挽回的损失。我们注意到供应商倾向于对更新、补丁和修补程序进行优先级排序。从《披露策略》的变化中可以看到，我们采用了适用于供应商的时间表，并使我们的流程与行业内类似的项目保持一致。

我们更新该政策的目的非常简单明确，即更好地与供应商和安全社区合作，一起尽可能多地缓解威胁。于所有人之中，我们明白每个漏洞都有它的独特性。

有关完整详细信息，请参阅以下链接中的官方政策文档：
http://www.cisco.com/c/en/us/about/security-center/vendor-vulnerability-policy.html

发布者：MITCH NEFF；发布时间：上午 10:02
标签：零日漏洞、CERT、披露、补丁、VULNDEV