Claroty 增强漏洞和风险管理功能 降低网络化物理系统(CPS)风险

2023 年 9 月 13 日
Claroty首席产品官
Grant Geyer 编写

虽然每个网络安全计划的目标都是降低风险，但资产密集型产业的风险会更高。如果这类企业的网络化物理系统(CPS)受到破坏，可能会对国家安全、经济安全和公共安全造成现实影响。只要看看过去几年众多针对医院、管道和水处理系统的勒索软件攻击事件，就可以得知CPS网络风险是当下真实且可怕的存在。

问题的核心在于：

1.为患者提供更好治疗效果的联网医疗设备、为企业实现更佳业务成果的数字化流程的CPS并未经过设计保护，容易受到网络攻击。

2.更糟糕的是，安全运营团队正在使用的标准和工具并不是为应对CPS网络风险而设计的。

2023年9月，Claroty宣布增强其xDome产品、Medigate平台的漏洞和风险管理(VRM)功能。Claroty xDome和Medigate是分别针对工业和医疗保健行业的SaaS解决方案。最新增强功能建立在目前已有的漏洞和风险管理功能的基础上，可进一步赋予关键基础设施资产所有者和运营商更有效的能力来克服CPS网络风险挑战。

以下讲述了企业正在面临的两大挑战和Claroty的针对性解决方案。

挑战 1：越来越多的CISO负责评估CPS网络风险状况

根据Fortinet发布的《2023年运营技术和网络安全状况报告》，在关键基础设施领域，超过95%的CISO不仅保护传统的IT环境，还要保护其CPS环境。而且，几乎所有CISO在向董事会成员和执行领导层报告时，需量化其CPS网络风险、说明风险状况。

尽管大多数网络风险评估解决方案有提供CPS网络风险评分，但在准确性和可操作性方面都存在缺陷。**考虑风险是对不良事件发生的可能性和影响的估计。在CPS网络安全方面，风险评估需反映：**

1. CPS被破坏的可能性有多大？

2. 这种破坏可能产生什么影响？

那么，准确地评估CPS网络风险状况，需要做到：

- **资产可视化：**传统的风险管理平台并不是为了对现有CPS和对重要业务提供可视化而构建的。如果没有对发现所需的大量协议和收集机制的支持，工具会对资产及其相关风险视而不见。

- **风险因素和补偿控制可视化：**每个CPS环境都有降低风险的潜力，以便操作员专注于未缓解的风险。分段、端点保护、访问控制和补偿控制等其他措施可以降低存在的固有风险。利用自动化来收集有关这些补偿控制的信息，并在风险计算中利用它们的能力对于专注于正确的风险敞口至关重要。大多数解决方案完全没有考虑CPS环境的补偿控制和风险因素，所以它们提供的风险评分往往过高，从而使安全运营团队面对的是大量已经缓解的问题。

- **可配置的风险框架：**尽管每个CPS环境和每个企业的风险承受能力都是独一无二的，但大多数解决方案提供的选项很少，无法根据客户的侧重点来自定义不同风险因素的权重。软件供应商开发固定风险计算是极其常规的，该计算无法根据企业所希望的风险计算来进行配置或调整。因此，大多数企业不能有效地利用风险评分功能来改善其CPS风险状况。

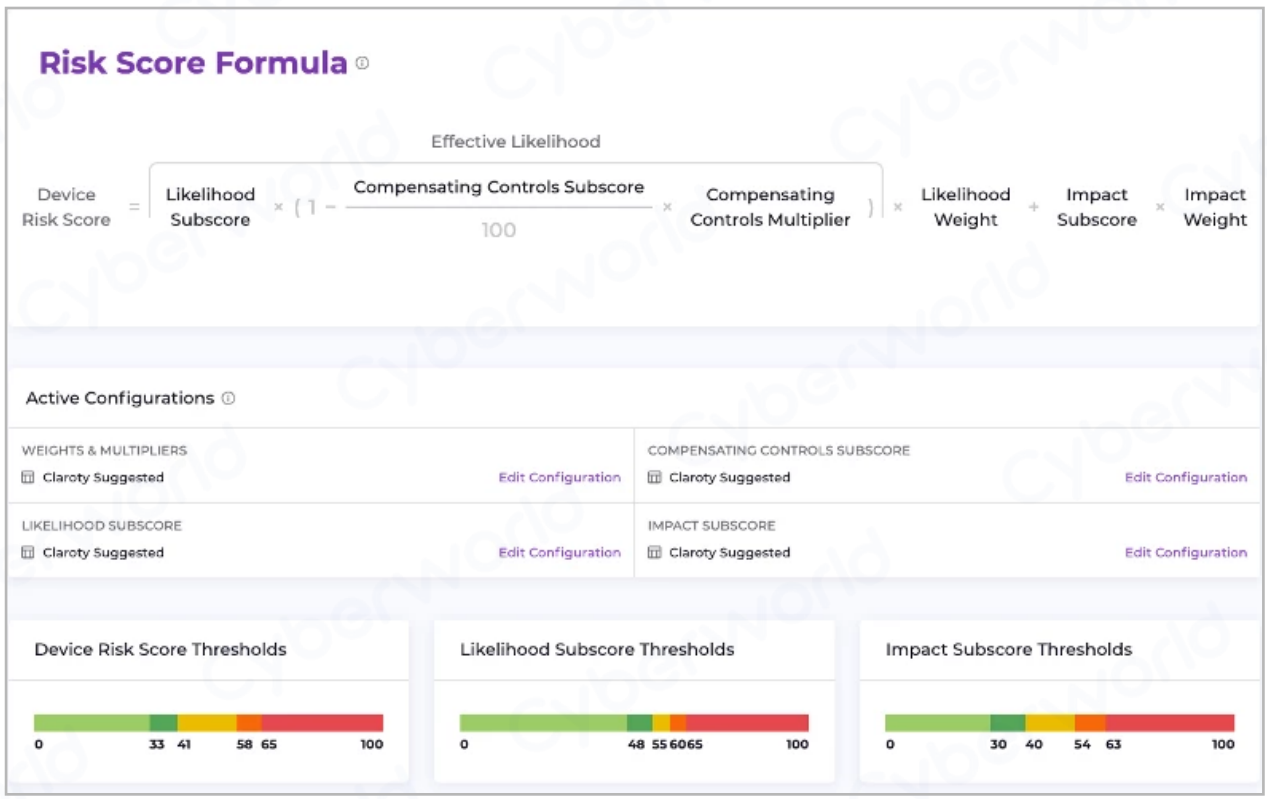
解决方案：Claroty的新风险框架可帮助CISO优化CPS网络风险状况评估

Claroty最新的漏洞和风险管理增强功能建立在业界领先的CPS可视化和发现功能的基础上，可进一步使CISO及其团队通过以下方式有效且高效地了解和量化其CPS网络风险状况：

提供业界最精细、最灵活的CPS风险评分框架

Claroty的新风险框架比以往更加准确，它考虑了更多可能发生的风险因素，以及可以抵消风险的补偿控制。这些功能是预先配置好的，开箱即用。因此，即使是刚刚开始使用CPS安全产品的客户也可以立即评估，并自信地采取措施改善其CPS风险状况。

Claroty的新风险框架也比以往更加灵活和可定制。**安全运营团队能根据自身需求定制CPS风险计算，将其与现有的治理、风险管理和合规审查流程保持一致，更好地控制不同因素在CPS风险态势评估中的权重。**



Claroty的风险评分框架经过预先配置，可反映每个客户CPS的独特安全性和业务环境。它也是可定制的，能够与任何现有的治理、风险管理、合规审查流程和风险定义无缝结合。

挑战 2：仅根据CVSS v3严重性评分确定修复漏洞优先级

在Claroty Team82发布的《2022下半年XIoT安全状况》报告披露的CPS漏洞中，将近70%的 CVSS v3 严重性评分为“高”或“严重”，但被利用的漏洞还不到 8%。

尽管存在这种差异，传统标准化解决方案还在建议基于 CVSS v3 严重性评分确定修复漏洞优先级。然而，2023年第三方研究[1]结果证实该建议是无效的。根据该研究，CVSS v3 引导的优先级：

- **平均覆盖率为82.4%：**“覆盖”指被优先利用的漏洞部分。这意味着，如果安全运营团队使用 CVSS v3 评分“高”或“严重”作为修复阈值，就会优先考虑其环境中82.4%的漏洞，而忽略其余17.6%的漏洞。

- **平均效率为3.9%：**“效率”指所有优先漏洞中被利用的部分。这意味着，在同一安全运营团队优先处理的所有漏洞中，只有不到4%的漏洞会被利用，而近96%修复资源将浪费在那些从未被利用的漏洞上。

如果安全运营团队仍遵循传统标准化解决方案——仅根据 CVSS 评分确定修复漏洞优先级，就会将资源错误地投入到最不可能被利用的漏洞上，而忽视了最有可能被利用的漏洞。

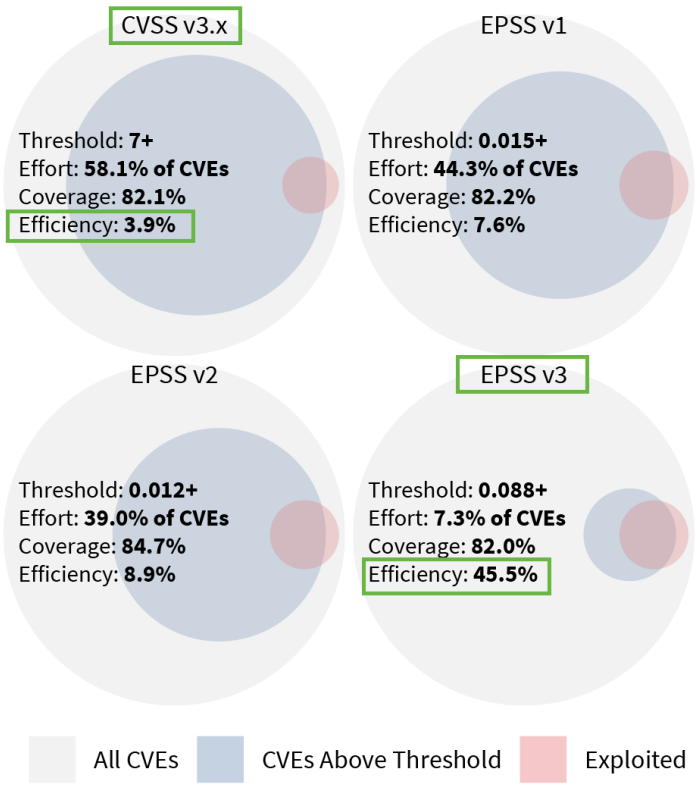
解决方案：Claroty根据利用可能性、资产重要性和影响，对漏洞进行优先级划分

Claroty最新增强的漏洞和风险管理解决方案进一步使CISO及其团队能够通过以下方式有效且高效地优先考虑影响其CPS环境的漏洞：

根据利用可能性，自动确定漏洞的优先级

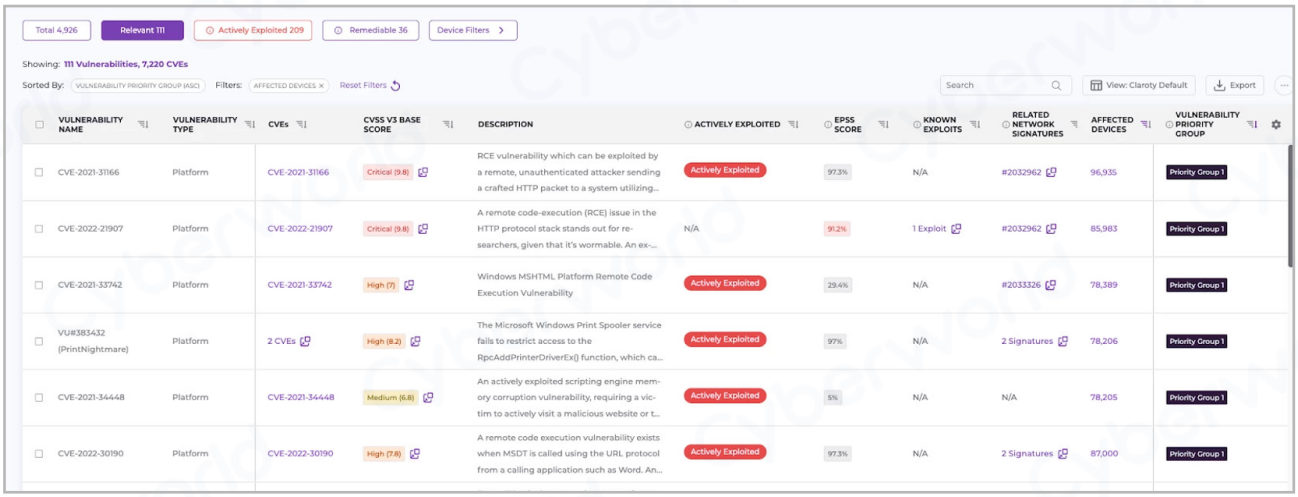
目前，**Claroty的漏洞和风险管理产品是业界第一个根据已知被利用的漏洞(KEV)目录、漏洞利用预测评分系统(EPSS)中最新状况和预测的可利用性指标，来丰富所有漏洞并将其分配到优先级组。通过跟踪所有已在野外被利用的漏洞，已知被利用的漏洞目录为那些已被武器化的漏洞提供了宝贵的见解。**与此同时，**漏洞利用预测评分系统使用数据科学模型来估计哪些漏洞可能在未来30天内被利用。**

结合这两个来源的最新数据点，Claroty能让安全运营团队全面了解对其自身环境构成最大风险漏洞的当前和近期状态。**安全运营团队可以更有效地（平均效率提高约11倍）优先考虑威胁行为者最有可能利用的漏洞。**



资料来源：Jay Jacobs 等五人于2023年6月发布的《增强漏洞优先级：通过社区驱动的见解进行数据驱动的漏洞利用预测》

如上图所示，**约 11 倍的效率提升是通过对比 EPSS v3 45.5% 的平均效率与 CVSS v3 3.9% 的平均效率来确定的。**它还强化了Claroty最新的漏洞和风险管理增强功能如何进一步帮助客户做出保护其最有价值资产的最佳决策。



Claroty根据最新的已知被利用的漏洞、漏洞利用预测评分系统可利用性数据，自动将所有CPS漏洞分配到优先级组，从而轻松了解和优先处理最有可能被武器化的漏洞。

基于整体资产风险，进一步优化缓解

每个漏洞优先级组内的CPS也通过Claroty之前提到的新风险评分框架得到了丰富。**此功能包括一个风险模拟器，使安全运营团队不仅能了解每个组中应优先考虑哪些CPS，而且还能了解是否应考虑现有控制措施、修补与补偿控制措施对风险的影响程度，以及反映每个环境中每个CPS独特上下文和漏洞的其他更深入的指导。**

Claroty增强漏洞和风险管理功能

- **新的风险框架**
- **新的漏洞优先级划分方法**

综上所述，Claroty针对CPS漏洞和风险管理的最新增强功能包括：

1. 提供业界最精细、最灵活的CPS风险评分框架。功能预先配置，开箱即用；客户也能根据自身需求定制CPS风险计算。

2. 根据利用可能性、资产重要性和影响对漏洞进行优先级划分，保护关键资产的效率提高约11倍。

随着CISO及其团队在管理CPS网络风险方面不断面临新的挑战，Claroty决心帮助客户减轻痛点，Claroty推出最新的漏洞和风险管理增强功能即可证明了这一点。最重要的是，**它能帮助客户了解其CPS网络风险状况，更好地分配现有资源来改进，并加速CPS安全之旅。**

如需了解此最新版本以及Claroty如何支持CPS安全之旅的相关信息，请联系Claroty的中国区总代理Cyberworld科明大同，获取Claroty xDome或 Medigate漏洞和风险管理解决方案简介。

注1：Jay Jacobs 等五人于2023年6月发布的《增强漏洞优先级：通过社区驱动的见解进行数据驱动的漏洞利用预测》

关于 Claroty

Claroty使工业、医疗保健和商业机构能够保护其环境中的所有网络化物理系统——扩展物联网 (XIoT)。Claroty平台可以与客户现有的基础设施集成，提供可视化、漏洞和风险管理、威胁检测、安全远程访问的全方位控制。Claroty得到了全球领先的工业自动化供应商的支持和采用，拥有广泛的合作生态系统以及屡获殊荣的Team82研究团队。

Cyberworld
广州科明大同科技有限公司

中国区
总代理

官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

CLAROTY