ivanti

解决方案概览

基于风险评估的 CVE 补丁列表审批

Ivanti 补丁管理解决方案中可用

Ivanti 提供记录漏洞扫描结果、查看已知公共漏洞和暴露 (CVE) 与相关补丁，以及发布或审批缺失的补丁部署等功能。

您的 IT 运营团队和 IT 安全团队需要承担不同的工作任务。运营团队需要确保设备都能顺利运行，而安全团队的职责是保障环境安全无虞。此外，这两个团队还有一个共同的目标，那就是在确保业务安全的同时为企业的发展助力。要想实现这个目标，他们必须在端点展开密切合作。

持续的漏洞评估和修复

持续的漏洞评估和修复应该成为企业安全实践中不可或缺的一部分。但是，从第一次发现漏洞到部署软件更新通常会花费巨大的时间与人力成本。

识别和修复一个漏洞不难，但当安全团队检测到数以千计的 CVE 时，漏洞修复将成为一项艰巨的任务。如果检测到 10,000 甚至 50,000 个 CVE 时，您又该如何应对呢？一次漏洞评估可能会在环境中的多个系统上发现相同的问题，或者同一漏洞可能出现在许多不同的系统上，也可能出现在同一系统上的许多软件中。

很快您就会发现，您工作的大多数时间都耗费在评估和修复各种漏洞上。而这段时间正好给了攻击者可乘之机，让他们有机会访问到您的敏感数据。处理漏洞花费的时间越长，发生安全事件的概率就越高。IT 运营团队必须仔细研究来自安全团队的报告，识别 CVE，将它们与已有的更新进行匹配，然后通过补丁管理解决方案将更新有针对性地推送给各个用户。

减少从识别 CVE 到分发补丁的时间

借助 Ivanti 解决方案中的“CVE 补丁列表”导入功能，您可以将这个过程从数小时缩短至数分钟。无论您使用的是 Rapid 7、Tenable、Qualys、BeyondTrust 还是其他供应商的漏洞评估，Ivanti 解决方案都可以找出与那些 CVE 相关的补丁，并构建一个可以进行快速审批或发布的补丁更新列表，让您可在环境中轻松开展修补任务。

导入已识别的 CVE 信息。Ivanti 的补丁解决方案能够通过这些信息找出与 CVE 对应的软件更新，帮助您有效解决漏洞问题。

进而，我们可以识别 CVE，将它们与解决这些特定漏洞的更新相匹配，并向您展示需要在各个端点上用到哪些补丁:

假设您的漏洞报告显示在环境中检测到 400,000 个漏洞。在报告中手动去重并找出所有的 CVE 唯一标识符 ID，可能需要花费数小时甚至数天的时间。而通过 Ivanti 解决方案将 CVE 与我们的补丁进行匹配，运营团队每次收到安全团队提供的新报告后，只需几分钟就可跑完这一流程。

如需了解关于这些功能的更多信息，请联系 ContactChina@ivanti.com。