持续的漏洞管理

对于一家企业而言，如果 IT 基础架构中的漏洞受到黑客们的攻击，那么其生产力、商誉包括经济上都会遭到巨大损害。网络安全应该是一个持续的过程，如果企业忽视了这一点，那么黑客便可以发现基础架构中存在的漏洞并将其作为攻击目标，然后在其中部署恶意代码并实施攻击，而且其攻击速度远快于安全团队的修复速度。今天看似安全的系统，下周就可能因为环境中的核心漏洞遭黑客攻击而瞬间崩溃。

在互联网安全中心看来，持续的漏洞管理能够“持续地获取、评估新信息并采取应对措施，进而识别漏洞、进行修复，大幅减少攻击者得逞的机会”。

持续的漏洞管理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，这对于任何企业而言都是一个不小的挑战。我们建议企业先加大漏洞扫描任务的频率，以免漏报。

安全团队在获取漏洞数据后，对其进行优先级排序，然后移交给 IT 团队，后者必须找到匹配 CVE（公共漏洞和暴露）的软件更新，并对更新顺序进行优先级排序。识别和修复一个漏洞不难，但如果有 10,000 甚至 100,000 个 CVE 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漏洞，或者同一漏洞可能出现在一个系统上的多个软件中。每次发现漏洞时，都需要通过去重和比对 CVE 来确定解决方法，而这个过程可能需要耗费 5 到 8 个小时的时间。一天可能看上去不算太长。但大多数的攻击发生在推出更新前的 14 到 28 天之间，因此每推迟一天，攻击者获得的攻击机会就越多。

缩短从漏洞识别到补丁部署的时间

Ivanti 的安全解决方案可让您获得更好的洞察力，并改善您的安全状况。通过对端点和服务器进行自动修补，让操作系统和第三方应用程序的补丁处于最新状态。我们的补丁解决方案与漏洞扫描程序、配置管理工具及报告工具相集成，可大幅提升 IT 与安全团队的工作效率。

实现持续的漏洞管理

我们的安全解决方案可简化漏洞的识别、分类、解决等流程，避免黑客去利用生成安全漏洞报告与采取修复措施之间的时间差。IT 团队可以轻松导入由安全团队获取的漏洞扫描结果。快速查看识别出的 CVE 和相关补丁，然后发布或审批缺失的补丁部署，进而节省大量时间。

无论是使用 Ivanti SCCM 补丁插件、Ivanti 端点管理器补丁插件来修补端点，亦或是借助 Ivanti 安全解决方案来修补数据中心，我们的 “CVE 补丁列表 ” 都可以助您一臂之力。

IT 团队以前需要在比对、去重和准备补丁组上花费大量时间，现在他们的体验和工作效率都已得到显著提升。用户可以轻松地从漏洞管理供应商那里导入任意格式的列表，比如 CSV、XML 或纯文本文件。然后自动将 CVE 与适当的软件更新进行匹配，以便更快地定位漏洞并了解需要应用哪些补丁。将环境中通过审批的补丁集合成组，还可以查看每个补丁的所有相关信息。

更好的洞察力，更出色的安全状况

您的 IT 团队需要花费多少天来研究、测试和分发补丁，您又如何对这些补丁进行优先级排序？通过公开文章、供应商文档和其他数据源中的已知问题来确定补丁更新的可靠性，同样非常耗时。而如果补丁推送的规则还是以关键补丁为先，而非那些正暴露给攻击者的漏洞补丁为先，那么潜在风险无疑会增加。

判断哪些补丁优先进行测试和分发，会进一步增加漏洞管理流程的复杂性。Ivanti 的智能修补工具，让您可以充分了解来自 Ivanti 第三方补丁目录的补丁数据，包括各补丁的可靠性和安全指标。通过获取以往需要耗费大量时间精力来挖掘的分析洞察，对重要更新的分发流程进行优化。

- **获取可见性**，充分了解供应商针对一个或一组补丁报告的问题，以及 Ivanti 在公告信息（包括相关 CVE 与补丁）中指出的问题。
- **加深洞察力**，通过分析客户是否需要回滚补丁的匿名数据，了解 Ivanti 客户所经历的共通性问题。
- **判断可靠性**，对更新及快速分发的可靠性进行研判。
- **发现补丁**，找出那些需要做更多测试的补丁，快速定位那些更新成功率更高的补丁，并根据威胁评分、可靠性评分来对测试和补丁部署进行优先级排序，优化修补流程。

利用 Ivanti 的持续漏洞管理解决方案，将黑客的攻击扼杀在摇篮之中。

如需了解更多信息，请联系 ContactChina@ivanti.com

了解更多

ivanti.com.cn
010 85412999
ContactChina@ivanti.com