Ivanti Neurons Patch for MEM (Microsoft Endpoint Manager)

利用基于风险的第三方补丁发布功能扩展 Microsoft Intune

Ivanti Neurons Patch for MEM 对现有 Microsoft Intune 实施加以扩展， 将第三方应用更新也纳入其中。 它的威胁和补丁情报能帮助企业对第三方软件漏洞修复工作加以适当排序。

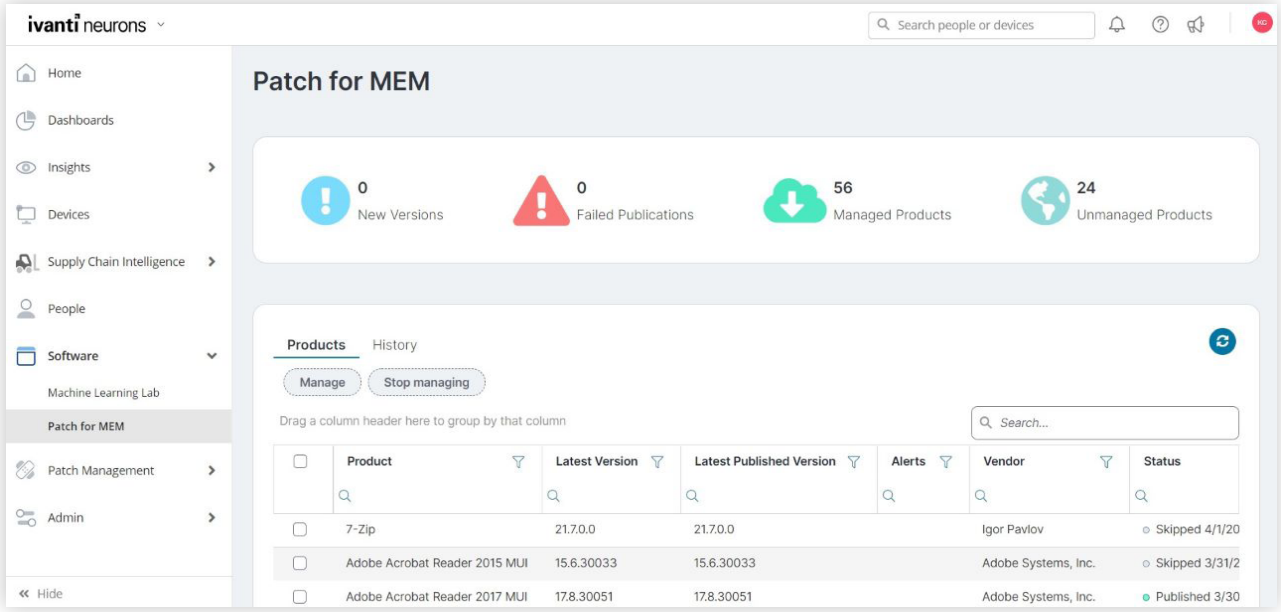
Intune 中的第三方应用更新

数据外泄和勒索软件攻击与年俱增。 同样，企业部署的应用数量也在增加，自 2016 年以来增加了 24%。[1] 因此毫不奇怪，第三方应用对网络不良分子来说已经成了最有吸引力的攻击途径之一。 遗憾的是，因第三方应用漏洞而造成的数据泄露也是代价极为高昂，使企业平均损失了 433 万美元。[2]

因此，企业需要勤于更新第三方应用，而随着他们必须考虑的应用数量不断增加，这可能成为一项挑战。 让问题愈加复杂的是，他们需要跟踪的漏洞数量也在不断增加——美国国家漏洞数据库 (NVD) 平均每天披露 61 个漏洞。[3]

好消息是，只有 4% 的常见漏洞和风险 (CVEs) 被公开利用。[4] 坏消息是，从 NVD 总共超过 13 万个漏洞中识别这 4% 的漏洞可能非常困难。 例如，如果企业根据常见漏洞评分系统 (CVSS) v3 来修补所有关键漏洞，那么他们将错失对 73.61% 的勒索软件漏洞的修补。[3]

对于那些利用 Microsoft Intune 向设备推送应用和更新的企业来说，这种情况可能更容易出问题。 虽然 Intune 为 Microsoft 应用提供全面的补丁管理功能，但它不具备更新第三方应用的原生功能。



引入 Ivanti Neurons Patch for MEM

Ivanti Neurons Patch for MEM 对现有 Microsoft Intune 实施加以扩展， 将第三方应用更新也纳入其中，并且无需任何额外的基础设施。 它提供实用的威胁情报和补丁可靠性洞见，使 IT 团队能够优先处理和修复对其组织构成最大危险的漏洞。 借助 Ivanti Neurons Patch for MEM，企业能够更好地保护自己免受数据外泄、勒索软件和其他源自第三方应用漏洞的威胁。

主要特色和功能

利用第三方补丁发布功能扩展 Microsoft Intune

实现 Intune 投资回报最大化，同时防范第三方应用漏洞所带来的威胁。 Ivanti Neurons Patch for MEM 从 Ivanti Neurons 云平台直接向 Intune 发布经预先测试的第三方应用更新。 这让 IT 团队能够将第三方应用更新作为现有应用生命周期管理工作流的一部分，随 Intune 内的 Microsoft 操作系统及应用更新一起得到部署。

此外，作为云原生解决方案，Ivanti Neurons Patch for MEM 让 Intune 客户能将其补丁工作负载完全迁移到云端，并实现 Microsoft 的现代化管理愿景，且无需任何额外的基础设施。

主动防范活跃漏洞攻击

根据敌对风险来确定补救措施的先后顺序，并提供关于已知漏洞的情报和漏洞威胁背景信息，包括与勒索软件的关联性。 与基本 CVSS 评分相比，Ivanti 的漏洞风险评级 (VRR) 通过采用最高保真度的漏洞和威胁数据以及渗透测试团队对漏洞的人工验证信息，能更好地帮助您根据风险情况采取优先行动。

避免补丁部署失败

通过经预先测试的应用更新和补丁可靠性洞见，节省时间并避免补丁部署失败。 Ivanti 对我们创建的每个补丁内容包都进行彻底测试。 测试是在一个广泛的虚拟环境中执行的，以确保该内容包适用于各类应用版本和操作系统，然后再将其发布至产品端。

为了进一步增强您的信心，来自公共社会情绪数据和匿名补丁部署遥测的补丁可靠性洞见使您能够在部署应用之前根据其在真实环境中的可靠性来评估应用更新。

简化补丁管理流程

利用 Ivanti Neurons Patch for MEM 的有用功能，实现一系列的操作效率：

- 当第三方应用有可用更新时，自动将其发布到 Intune 中（自动发布可选）。
- 利用经预先测试的应用更新，配合补丁可靠性洞见，让修补工作更可靠，减少部署失败情况。
- 利用威胁情报有效地确定修补工作的先后次序，这样您就能够专注于真正重要的漏洞。
- 利用漏洞和恶意软件洞见，促进安全和 IT 运营团队之间的数据及风险对话，从而改善运营协作。

关于 Ivanti

Ivanti 让无处不在的工作空间成为可能。 在无处不在的工作空间，员工使用各种各样的设备访问 IT 网络、应用和数据，以便能够在任何地方保持工作效率。 Ivanti 自动化平台连接业界领先的统一端点管理、零信任安全和企业服务管理解决方案，通过单一操作窗口让企业能够为设备提供自我修复和自我保护服务，并为最终用户提供自助服务。 已有超过 40,000 家客户，包括 96 家财富百强企业，选择了 Ivanti 来为他们发现、管理、保护和服务从云端到边缘的 IT 资产，并为员工提供卓越的终端用户体验，无论他们在哪里、用什么方式工作。 更多信息请访问 ivanti.com.cn。

ivanti

ivanti.com.cn
8610 85412999
ContactChina@ivanti.com

1. Okta, “Business at Work 2022 Report”, 2022. https://www.okta.com/report/businesses-at-work-2022/
2. IBM Security, “2021 Cost of a Data Breach Report”, 28 July 2021. https://www.ibm.com/security/data-breach
3. Cyber Security Works, Cyware, Ivanti, “2022 Ransomware Spotlight Report”, 26 January 2022. https://www.ivanti.com/lp/security/reports/ransomware-spotlight-year-end-2021-report
4. Cybersecurity and Infrastructure Security Agency (CISA), “Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities”, 3 November 2021. https://cyber.dhs.gov/bod/22-01/