Ivanti Neurons for Patch Management

有效地对漏洞加以排序和修复

Ivanti Neurons for Patch Management 是一个云原生的补丁管理解决方案，能够智能化辨识活跃风险漏洞、补丁可靠性和设备合规性、健康及风险并提供可行的修补措施，帮助企业更好地防范包括勒索软件在内的各种威胁。

基于风险的补丁管理

勒索软件攻击的频率和严重程度 与年俱增 这给公司带来了极为严重的影响。研究表明，勒索软件漏洞的平均总成本为 462 万美元——不包括赎金成本。[1]

不幸的是，情况可能还会变得更糟。勒索软件即服务 (RaaS) 使任何人都能发起攻击——不需要安全知识或编码专业技能。除此之外，网络中常见漏洞和风险敞口 (CVE) 的数量在 2020 年几乎翻了四倍。[2]更糟糕的是，勒索软件攻击者越来越多地把目标瞄准中型市场公司，以避免攻击大型企业所带来的媒体关注。[3]

打补丁修复 CVE 是组织抵御勒索软件攻击最该做的事情之一。很遗憾，71% 的 IT 和安全专业人士 发现打补丁太过复杂和耗时。[4]这可能是因为现存的漏洞数量 实在过于庞大。美国国家漏洞数据库 (NVD) 中就列出了超过 100,000 个漏洞。虽然仅有一小部分与勒索软件有关联，活跃漏洞所占的比例还要更少，但要识别其中哪些会对您的组织造成最大风险可能是件很麻烦的事情。从 2018 到 2020 年，使用CVSS v3 评分标准的话，如果您仅能为重大漏洞打补丁，那么您防范勒索软件的能力将仅为 35% 左右。[2]

Ivanti Neurons for Patch Management 提供实用的威胁情报、补丁可靠性分析和设备风险可视性，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。通过利用 Ivanti Neurons for Patch Management 来提高补丁工作的效率和效果，企业可以更好地保护自己免受数据外泄、勒索软件和其他源自软件漏洞的威胁。

主要特色和功能

主动给活跃漏洞打补丁

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 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。

借助对补丁可靠性和变化趋势的分析认知，实现更快的 SLA

从来自社会大众的反馈调查数据和对匿名补丁部署的结果中获得对补丁可靠性的深入认知，从而节省时间并避免失败的补丁部署。这些信息使您能够在部署补丁之前，根据它们在现实应用中的可靠性对其做出评估。此外，服务水平协议 (SLA) 跟踪——它提供了哪些设备能符合 SLA 指标的可见性——使您能够在设备不合规之前对其采取行动。

从本地过渡到云端补丁管理

借助 Ivanti 在补丁技术上的实力，开始您从本地补丁管理过渡到云端的旅程。Ivanti Neurons for Patch Management 是一款云原生解决方案，它让您能够按自己的步调逐步从本地补丁管理过渡到云端补丁管理，而不是强行“剥除并替换”。该解决方案让您能通过单一控制面板清楚查看它在云端管理的那些设备以及通过本地 Ivanti 补丁管理解决方案管理的那些设备，从而实现了上面这种渐进过渡。

简化补丁管理流程

通过消除在彼此孤立的补丁管理解决方案之间来回切换的需要，提高运营效率。Ivanti Neurons for Patch Management 让您能够通过单一控制面板清楚查看环境中所有端点设备。通过先进的漏洞发现与分析技术和补丁情报使您能够有效地确定补丁工作的先后次序，以便您专注于重要任务，从而进一步提高了运营效率。此外，当需要打补丁时，部署在设备上 Ivanti Neurons Agent 中的自主补丁配置程序会在几分钟内向数千台机器分发经过全面测试的补丁。

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”中，员工使用数不清的设备访问 IT 网络、应用和数据，以便能够随时随地保持工作效率。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 78 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。

版权所有 © 2022, Ivanti. 保留所有权利。IVI-2652 02/22 RW/DH/MM

ivanti neurons

ivanti.com/neurons
1 800 982 2130
sales@ivanti.com

1. IBM Security, “2021 Cost of a Data Breach Report”, 28 July 2021. https://www.ibm.com/downloads/cas/OJDVQGRY
2. RiskSense, Cyber Security Works, “Ransomware Through the Lens of Threat and Vulnerability Management”, 9 November 2021. https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensecsw
3. Coveware, “Ransomware attackers down shift to ‘Mid-Game’ hunting in Q3 2021”, 21 October 2021. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
4. Ivanti, “Patch Management Challenges: Survey Results and Insights as Organizations move to Everywhere Workplace”, 7 October 2021. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges