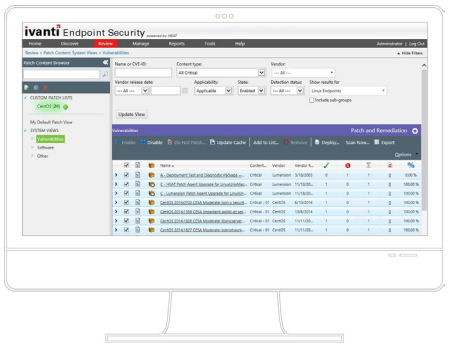
保护您的异构环境

如今，混合操作系统环境盛行，要应对此环境的补丁问题，您的工具箱怎能少了补丁管理软件。而要想实现有效管理，只能处理 Windows 补丁远远不够，还必须能处理多种操作系统的补丁。此外，如能使用单个界面和自动化工具高效进行管理，则不仅可以释放 IT 资源，还可以在增强防御的同时减少人为错误。



补丁修补 — 有效保障安全的基础

网络攻击越演越烈。为应对这一局面，企业制定出各种计划来强化自己的安全防护。如论及构建有效的多级安全策略，毋庸置疑，企业首先要考虑的便是补丁修补。但补丁修补仍存在诸多问题。威胁“制造者”仍可利用本可以通过补丁消除的漏洞继续发起进攻。

不仅如此，如果采用的是耗时的手动工具，那么不仅会减少 IT 人员为业务目标提供支持的时间，还会让他们的出错几率升高，从而导致补丁修补工作费心费力却收效甚微。而在异构环境中，情况只会变得更糟糕，因为 IT 人员使用的修补工具非常多。

Ivanti® Linux、UNIX、Mac 补丁插件由 HEAT 提供支持，可迅速检测当今环境中的漏洞，覆盖范围从工作站延伸至数据中心。此外，此工具还可自动部署预先经过专家测试的补丁，帮助企业提高补丁修补的效率和效果。

把基于代理的补丁修补应用到 Windows 操作系统以外

借助能够为 Linux、UNIX 和 Mac 提供修补支持的工具，保护数千个系统和来自数百家供应商的第三方应用程序。此控制台内置自动化功能，可降低出错的风险，也可简化修补混合环境的流程。

自动进行漏洞评估和补丁管理

补丁修补不在一劳永逸，而在不断改进。Ivanti Linux、UNIX、Mac 补丁插件具备可按需使用的智能排程功能，能够轻松发现环境中的漏洞。此工具会不断更新补丁信息，也会把新信息用到评估当中，如有需要，还会自动修复系统漏洞。此外，此工具支持管理及控制部署任务，可以在不中断用户和核心基础设施的情况下完成修复。这样一来，企业再综合自己的合规性报告结果，便能清楚地看到当前面临的风险。

帮助确保合规性

监控、评估并保护您的工作站和服务器，确保设备均符合 PCI、HIPAA/HITECH 等安全标准。合规性得到保障后，既可以避免罚款，又可以节省时间和资源。

保障用户生产力

补丁修补不一定会影响用户生产力。选对修补时机，把握好修补条件，您的业务完全可以在不影响安全性的情况下蓬勃发展。

增强安全团队与 IT 运维团队间的协作

Ivanti Linux、UNIX、Mac 补丁插件可以与安全信息和事件管理 (SIEM) 系统集成，增进安全团队对运维工作的了解。

这种集成还有助于增强安全团队、IT 团队与 DevOps 团队间的协作。举例来说，出现风险时，风险管理和风险登记系统可以接收漏洞和补丁信息，以便对漏洞进行持续评估。此时，具备强大补丁管理解决方案的 DevOps 团队，则可主导基础设施与系统的优化工作，提高灵活性、耐用性和一致性。

- 工程和质量保证团队可以确保环境中补丁修补和第三方库的一致性，从而增强部署的稳定性。
- DevOps 团队可以实现补丁和第三方库的部署自动化，确保安装的一致性，进而减少部署过程中的人为错误。
- 集成的报告功能可显示汇总信息、当前状态汇总和偏离规定修补级别的配置，让各个团队都受益。

主要功能

- 基于 Web 的控制台，具备集成的报告和警报功能
- 集中的补丁部署
- 基于策略的配置、评估和补丁部署
- 实时的定制化报告
- 全面的补丁目录

www.ivanti.com.cn

010-85153668

ContactChina@ivanti.com