TREND MICRO™ 趋势科技

全程护航
迈向云端

趋势科技™

漏洞屏蔽

补丁管理面临的挑战

当今企业面临的威胁形式严峻而又复杂，Duqu 和 Conflicker 等恶意程序将攻击的矛头直接指向企业最为倚重的系统中的漏洞。不计其数的软件漏洞为数据窃取恶意软件和其他攻击留下了方便之门。IT 团队无法及时修补这些漏洞 — 在漏洞被利用之前，根本不可能针对所有高危漏洞下载、测试和部署补丁。而且，紧急修补将导致停机、开销过大和成本过高等不愉快的使用体验；虚拟化将带来其他操作挑战；PCI 规则要求在 30 天内强制安装补丁；零日攻击频率不断增加。这些挑战警示我们，寻找一种虚拟补丁解决方案，进而通过屏蔽已知和未知漏洞补充现有补丁管理流程迫在眉睫。

主要驱动因素

- Microsoft Tuesday
- PCI 6.1：安全补丁
- Oracle 补丁技术
- 虚拟化

“他们的补丁管理流程有效率仅为 27%。”

《信息周刊》

哪里最容易受到攻击？

企业需要屏蔽大量关键应用程序和系统中的已知和未知漏洞，以使网络犯罪分子无的放矢。

企业应用程序：每年都会报告操作系统、数据库、服务器和其他应用程序中存在的数以千计的高危软件漏洞。修补这些漏洞可能导致破坏性后果并浪费大量时间，需要重启系统并会影响服务水平协议。即使在有补丁可用时，也需要数周甚至数月的时间才能将补丁完全部署好。

旧版本 Web 应用程序：绝大多数违规记录都是由 SQL 注入攻击 Web 应用程序导致的。Web 应用程序之所以成为众矢之的，是因为其本身具有开放特性并且可供攻击者访问。此外，随着内容和功能变得越来越复杂，程序员经常是未经培训就参加到安全软件开发实践中。外围安全设置无法屏蔽这些系统，找到并分配修复代码所需的自定义开发资源难度也很大。

不受支持的操作系统和应用程序：Oracle 10.1 和 Solaris 8 等旧版操作系统和应用程序到期之后，针对其开发或发布补丁的工作随之停止。通常，迁移至新版本的时间和费用太高，公司需要更直接、更经济有效的解决方案。当对 Windows 2000 的支持于 2010 年 7 月结束之后，作为一种经济有效的方式，虚拟补丁技术成为确保上述系统和其他不受支持系统获得持续防护的唯一选择。

无法安装补丁的系统：一般来讲，销售点设备、展台以及医疗或其他嵌入式设备是无法安装补丁的。因为远程位置之间的低带宽通常会使部署大型补丁要么耗时惊人，要么成本极高。此外，规则或服务水平协议的正常运行时间要求可能会阻止系统安装补丁。

趋势科技服务器深度安全防护系统提供漏洞屏蔽功能

趋势科技服务器深度安全防护系统可以在提供并部署漏洞之前屏蔽关键系统中的漏洞，也可以代替可能永远无法实现的补丁进行安全防护。无论以哪种方式，都可以显著降低成本和服务中断次数，使您可以更好地控制补丁的安装进程，进而在短时间内以较高的成本效益完善传统补丁安装流程。趋势科技服务器深度安全防护系统旨在为所有服务器（物理、虚拟和云）和某些端点提供全面防护，您可以将其部署为物理或虚拟机上的客户端或 VMware ESX 服务器上的虚拟设备，以保护客户虚拟机。

主要功能和优势

- **入侵检测和阻止 (IDS/IPS)** 规则可防止攻击者利用已知漏洞。趋势科技服务器深度安全防护系统可针对包括数据库、Web、电子邮件和 FTP 服务器在内的超过 100 款应用程序提供全新的漏洞防护。此外，IDS/IPS 规则还可以为尚未发布补丁的已知漏洞和未知漏洞提供零日防护。
- **建议扫描**可简化安全更新管理，方法是通过自动扫描系统推荐保护特定系统所需要部署的规则。趋势科技服务器深度安全防护系统在扫描系统后，会根据操作系统版本、Service Pack、补丁级别和安装的应用程序确认要实现最佳防护需要部署哪些 IDS/IPS 规则。趋势科技服务器深度安全防护系统还可以自动建议何时删除规则以最大限度降低资源影响。
- **安全更新**由一个专门的安全专家团队提供，该团队持续监控多个漏洞信息泄露源，可以识别和关联新的相关威胁和漏洞。趋势科技还可以先于 Microsoft 的每月安全公告收到他们提供的漏洞信息，使预测紧急威胁和提供更加及时的防护成为可能。
- **Web 应用程序防护规则**可抵御 SQL 注入攻击、跨站脚本攻击和其他 Web 应用程序漏洞，进而在完成代码修复之前屏蔽这些漏洞。安全规则强制实施协议一致性，并使用启发式分析识别恶意活动。
- **企业级双向状态防火墙**允许通过正确服务器操作所需的端口和协议进行通信，并阻止所有其他端口和协议。这可以降低未经授权访问服务器的风险。
- **物理、虚拟化和云计算环境防护**的屏蔽功能很强大，无论主机的部署方式为何都可以将漏洞拒之门外。除了提供基于客户端的防护之外，趋势科技服务器深度安全防护系统可利用 VMware API 提供具有虚拟化感知能力的防护，从而最大限度提高部署灵活性。

为漏洞屏蔽选择正确的解决方案

凭借超过 20 年的安全经验，趋势科技是提供虚拟补丁修复解决方案的领先企业。我们可以通过适合您企业的安全方案帮助您在最大限度降低复杂性的同时实现最佳防护。

有关详细信息，请访问 www.trendmicro.com/virtualpatching

聚焦 Conficker

趋势科技服务器深度安全防护系统帮助用户阻止了以 Microsoft Windows 2000、Windows XP 和 Windows Server 2003 (MS08-067) 中发现的高危漏洞作为目标的攻击，此次阻止发生在该漏洞被公布的当天，而 Conficker 利用其发动首次攻击发生在数周之后。

桌面漏洞屏蔽

趋势科技入侵防御防火墙可屏蔽 Windows 台式机和笔记本电脑中的漏洞，并可以无缝插入趋势科技防毒墙网络版控制台进行一体化管理。

> “在补丁可以部署之前，趋势科技服务器深度安全防护系统通过主动屏蔽电子健康记录 Web 应用程序和操作系统中的漏洞保护我们的医疗系统。”
>
> **Bill Gillis**
> Beth Israel Deaconess Medical Center