Ivanti 白皮书

软件补丁和更新：IT 安全的安全带

ivanti

目录

简介 3
补丁：价值明显，然而部署不一致 3
为何程序修补仍混乱不堪 — 以及如何解决这一问题 4
Ivanti® 补丁管理器如何帮助您 5

与销售沟通：

010-85153668 转产品咨询

访问我们的网站 www.Ivanti.com.cn。

简介

几乎所有轿车和有座位的商用车辆都配备了安全带。而数不清的研究也证实，安全带可以保护生命并减少与车祸相关的伤害。例如，根据美国疾控中心 (CDC) 的研究，“安全带几乎可以减少一半因车祸导致的严重伤害和死亡。”根据 CDC 的估计，有这样一个醒目的数字，“在 2012 年，有超过 220 万名成年驾驶员和乘客因为机动车事故受伤而接受急诊治疗”并且同年“因非致命车祸伤害而产生的医疗和误工费用超过 500 亿美元”。

但遗憾的是，每年在机动车事故中，仍有不小比例的人因为没有系安全带而死亡或严重受伤。

想象一下，如果并非所有车上都配置有安全带，那么死亡和受伤的比率将会高出多少；如果每位机动车主都必须研究和比较不同安全带解决方案，选择一个，购买它，安装它，然后确保它工作正常并保持最新，情况又会如何?

如果面临这么多挑战，是不是可能大部分机动车主都会跳过这方面的开支和麻烦，然后在不配备安全带的情况下就开车上路？显然并不太可能出现这种情况，因为大家都了解，如果没有安全带，驾乘风险将增加许多倍。

但由于一系列原因（这些原因与逻辑或财务都没有关系），许多企业仍不愿投资在程序修补自动化和相关流程上。不知为何，这些企业的管理层认为继续在明知不受保护或保护力度不够的系统上开展业务，比起充分保护这些系统更为经济而方便，即使他们了解风险的大小，也看到了同行公司由于类似风险而遭受的明显严重后果，他们仍固执己见。

补丁：价值明显然而部署不一致

就有效的 IT 安全而言，对主动性修补流程（以及支持该流程的工具）的重要性怎么高估都不为过。澳大利亚信号局（Australian Signals Directorate，澳大利亚国内类似于美国国家安全局的机构）估计，至少有 85% 的针对性网络攻击可以通过四个简单的步骤加以预防。

- 应用程序白名单
- 修补应用程序
- 修补操作系统
- 限制管理权限

显然，程序修补的价值在安全领域专家的人群中得到了广泛的认可。2015 年 7 月，Google 发布了基于针对 231 名网络安全专家和 294 名“典型互联网用户”如何保护自己的重要数据的调查研究结果。在专家中，安装软件更新是被提到最多的保护措施，甚至位于设置高强度密码和双因素身份验证之前。35% 的专家组受访者将软件更新列为重要的措施，而非专家组则仅有 2%，他们更多地将精力放在防病毒软件和高强度密码上。

在许多情况下，有效的程序修补不仅仅是值得尝试的手段，甚至可以说是开展业务的必要条件。如同 HP 在 2015 年 6 月的安全简报“The hidden dangers of inadequate patching”（程序修补不完全所带来的隐形危害）中所指出的那样，“行业标准以及各种政府法规的合规性同样需要一套稳健的服务和程序修补战略。”要求补丁管理的法规包括支付卡行业数据安全标准 (PCI DSS) 以及欧洲网络和信息安全 (NIS) 指令。

虽然对于安全工作有着显而易见的价值，但程序修补在很大程度上仍是一个亟待解决的问题。Verizon 2015 年的数据违规调查报告 (DBIR) 发现“被利用的漏洞中有 99.9% 都是在公共漏洞列表 (CVE) 发布超过一年之后才遭到攻击的。”更令人不安的是，就在这份报告中还发现，“许多现有漏洞仍然门户大开，这主要是因为早就可用的安全补丁从未得到实施。实际上，许多漏洞可以追溯到 2007 年，这期间几乎有 8 年时间。”

而在美国计算机紧急响应小组 (US-CERT) 于 2015 年 4 月发布的警报中列出了 US-CERT 发现的“30 大针对性高风险漏洞”。与这 30 项漏洞相关的、最早的 CVE 和安全公告是在 2006 年。

为何程序修补仍混乱不堪 — 以及如何解决这一问题

如同之前提到的 Google 研究中所述，“软件更新…是在线安全的安全带，它们让您在一段时期内更安全。可是，许多非专家人员不仅没有将这视为一项最佳实践，反而还错误地认为软件更新存在安全风险。”

这是不是一个错误，这也是一些专家共同担心的问题之一。对于为何关注安全的业务人员不进行程序修补或不信任补丁的原因，HP 的研究强调了以下几条：

- 补丁会打破既有的事物
- 补丁会引入安全问题
- 补丁不会按照预期的正常工作
- 补丁包括一些没有记录在文档中/不需要的“奖励功能”
- “静默”补丁部署通常会打扰用户，或扰乱故障排除工作

除了这些担忧之外，如何发现所有需要或可能需要修补的系统并排定优先级也可能是一项难度极大的工作。而为了给移动设备、远程办公或流动的 IT 用户提供支持，这些工作的难度可能还会加大。

幸运的是，现代的补丁管理解决方案解决了上面列出的所有问题。例如，补丁在交付到您的企业之前会经过彻底测试和检查，不太可能会打破既有的事物，引入安全问题，无法按照预期的正常工作，或是包括不需要的功能。充分可配置的补丁管理解决方案可以在不打扰用户或中断业务运营的情况下交付补丁。而现代化的解决方案可以针对您企业的所有重要操作系统和第三方应用程序提供补丁的部署和管理功能。

对于需要保护较大、较复杂环境的用户而言，通过建立以业务为驱动的补丁优先级，从而实现一致管理的方法非常有用。该方法的开发和执行都必须以特定的业务需求和目标为基础。但是，并不需要从零开始创建它们。例如，Forrester Research 为其客户提供称为“优先修补流程”(prioritized patching process, P3) 的一套方法。

在其 2014 年 2 月的新闻稿中，ISACA 在“4 Considerations During the Patch Management Process”（补丁管理流程中需要考虑的 4 个因素）一文中提供了流程的摘要。

1. 通过使用预测威胁建模来评估攻击的难度，从而确定您最易受到攻击的资产，并预测出攻击它们的难度。
2. 衡量漏洞对每项资产的潜在效果，其基础一部分基于资产上保存的数据的类型和敏感性，另一部分则基于资产所访问的数据的类型和敏感性。
3. 考虑每种漏洞是否已有被利用过的实例存在，以及这种利用行为的恶意程度，衡量这种被称为每个漏洞的“内在风险”。
4. 按照三种建议的估算和衡量指标，根据风险分类和评估来指定补丁的优先级。

所有这些都是实现有效的补丁管理的基本要素，但仅仅是整个流程的一部分。HP 的研究确定了另外几个必要的步骤。

1. 准确、完整地发现所有资产
2. 确定哪些资产需要保护，以及需要使用何种流程来保护每项资产
3. 确定可靠的供应商来提供所需的补丁并展开稳定合作（这可能需要订阅到电子邮件列表或在社交媒体上关注供应商）
4. 根据各种因素，比如员工配备和自动化解决方案成本、补丁失效率以及部署所需时间等，确定如何最好地安装和管理所需的补丁

还有许多来源可以提供其他的补丁优先战略和执行建议的示例 — 从研究公司到补丁管理解决方案供应商及其集成商合作伙伴，都可以提供这些示例。但是，即使不用到任何这些资源，您也很可能可以自行大幅改良自己企业中的补丁管理流程。努力针对最关键的系统和应用程序去确定、评估、部署和管理补丁，做出比今天更为一致的程序修补工作，这就是一个良好的开端，并最终将实现更好的程序修补。

是的，补丁可能会破坏既有的事物或影响用户的工作效率。是的，有时候补丁甚至会引入新的安全漏洞。但是所有这些都不能成为不及时全面应用补丁的理由。实际上，这些困难和其他争论都强烈需要通过主动的、战略的、可操作方法来进行补丁管理，并在更广泛的意义上改进 IT 安全性。该方法首先要开发并精炼一套流程，用于对补丁进行一致而有效的优化和实施，然后选择最适合于实施这些流程的工具。

全面有效的资产、系统和服务管理需要全面可靠地保护这些资产、系统和服务。而全面有效的、以用户为中心的安全则要从全面有效的补丁管理开始。

Ivanti® 补丁管理器如何帮助您

安全带结合保护，共同为您保驾护航，让您实现所追求的目标。Ivanti® 补丁管理器组合了您所需的功能，可在企业中实现全面、统一的自动化补丁管理。检测和修补 Microsoft Windows、Mac OS 以及所选 Linux 操作系统的漏洞。修补数百种类型和版本的第三方应用程序，比如 Oracle、Java 以及普及率高的 Web 浏览器。

建立一致的程序修补策略并自动化实施，不管企业资产是移动设备、远程设备还是处于睡眠状态，都可以轻松应对。在几分钟内完成数千套系统补丁的测试、打包、暂存和部署。使用灵活的报告和仪表盘来查看更多，了解更多并保护更多，还可以通过他人能够理解和使用的格式与他人共享信息。

相对于存在诸多限制的手动流程而言，Ivanti 补丁管理器可以帮助企业自动化和简化补丁管理并节约金钱。美国某家地区性银行每年可以节约超过 20 万美元。

请垂询您的 Ivanti 代表了解更多信息，或在线访问 www.Ivanti.com.cn。