快速防护能否应对零日攻击？微软力推Fixit思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_BF_AB_E9_80_9F_E9_98_B2_E6_c101_644070.htm 面对最近针对ActiveX控件的猖獗的零日攻击，微软正在迅速的展开反击，意图将短期快速修复技术纳入到其整体补丁管理工具箱的更新中，阻止恶意软件利用漏洞发起攻击。微软这次使用的武器是今年1月份推出的Fix-it技术。 Fix-it的代码可以为新出现的漏洞提供即时的保护，直到补丁开发完成通过测试。 Fix-it属于MSI文件，安装之后会通过改变注册表的设置来关闭带有漏洞的ActiveX控件。Fix-it文件允许系统管理员安装、维护和删除操作系统中的软件。“ 我们在想办法如何能够更好地将Fix-it技术与其它的微软补丁集成起来， ”负责了大部分Fix-it技术工作的微软支持与服务团队产品经理Paul Schottland说。 1月份以来，微软已发布了300多个Fix-it，其中大多数是为非专业人员而服务的，比如解决恢复误删除IE快捷方式和修复声音系统等小问题。但最近，Fix-it的重点转向了安全漏洞。51CTO编者按：以前微软在测试补丁期间，是不管外面攻击泛滥的。最多给个临时解决方案，这次改动，微软算是更加务实了。“ 我们要走的道路是找到整个行业的最佳做法， ”Schottland说，“ 我们要确保这个新的工具能够适应我们所管理的全部企业软件。 ”微软计划在下月份发布白皮书来描述这一战略。 Schottland说Fix-it技术并不适用于每个安全漏洞，但是当某些功能需要开启或关闭时，它可以发挥良好的作用，而不用让用户一直等着发布补丁。 上周早些时候，微软为Office Web 组件的ActiveX漏洞发布了Fix-it技术

“ kill-bits ”。据微软说该漏洞的补丁仍处于开发阶段。微软同时还发布了针对另两个 ActiveX控件零日攻击的kill-bits。在上周二，微软发布了第一份“ kill-bits ”的集合补丁MS09-032。 虽然kill-bits行之有效，但对于企业来说，主要问题是要让它们能够自动化进行。现在的Fix-it技术主要还是通过微软网站来手工操作。Fix-it技术主要是针对普通消费者，而一些防病毒厂商已经开始为企业用户提供集中管理Fix-it代码的工具。 微软建议使用它的系统中心配置管理器(System Center Configuration Manager)或使用Active Directory的群组策略功能来通过网络接收Fix-it代码。Schottland的团队正在与微软安全响应中心合作，与Windows Update团队共同开发快速部署的企业解决方案。 微软允许IT管理员下载Fix-it MSI文件，在内部网络中安装而不需要终端用户亲自操作。“ 管理员们可以使用登录脚本、组策略或配置管理器来完成安装， ”Schottland说。另外OEM厂商们也得到准许使用MSI软件包。“ (Fix-it)是不是将成为安全补丁的另一种途径?当然。 ”Schottland说。安全专家们认为，微软走在保护用户的正确轨道上，禁用ActiveX的行动是一个快速的解决方案。“ 微软的新技术是完全正确的， ”Shavlik Technologies首席技术官Eric Schultze说，“ 在以前的日子他们只是在等待每周二的补丁。而他们现在有办法在24小时内扭转情况，这是很了不起的。现在的问题是他们能否让IT管理员们操作起来更容易，我认为他们能做到。 ”Schultze说他们公司已经开始给客户提供集成了Fix-it软件包的补丁管理工具。 但是，零日攻击的攻势一波高过一波。安全厂商Qualys首席技术官Wolfgang Kandek说， 在Qualys的数据库中已经列出了60项零日攻击，

而在其他厂商那里已经超过了100项，“我不认为零日攻击的趋势会在短期内结束。”Kandek说，有趣的是最近这些零日攻击的目标指向了ActiveX，试图从网页攻击本地的计算机。Java Applets也有类似的危险，但它们并不像ActiveX这样直接控制操作系统，所以看上去没有那么可怕。问题涉及的不仅仅是微软。Mozilla提示用户在Firefox3.5中禁用Just-in-time(JIT)JavaScript编译器，为了在漏洞补丁发布之前避免零日攻击。而Adobe也在上个月发布了PDF零日漏洞的补丁。Google正在开发称为Native Client的技术，用于在准备中的Chrome OS中提高Web应用的本地处理性能。Google的工程师承认这项技术可能是“大胆而冒险的”，并正在努力提高安全性。