解读路由开发：高价值大投入思科认证 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__E8_A7_A3_E8_AF_BB_E8_B7_AF_E7_c101_644143.htm 控制着如此多的网络流量的路由器已经证明远程入侵者想进行破坏不是件容易的事情，这听起来似乎有些违反常理。德国一家安全实验室的研究所在Black Hat安全会议上声称虽然路由的开发利用是较高的目标，但是已经涌现出大规模的先进开发。 之所以是较高目标，部分原因是受到路由器本身属性以及广泛部署的路由操作系统(思科 IOS)两方面的限制。 路由器不会向攻击者暴露许多功能。路由协议在内部运行。此外网络设备中的弊端通常是作为功能问题被修复的，因为它们要求高度的可用性。 当前将侧重点放在客户端的缺陷上的策略也保护了路由器，因为它们很少会以客户端方式运行。 思科IOS身上某些明显的缺陷也为攻击增加了难度。来源：www.examda.com 思科不能从软件中出现的任何错误恢复过来。对于错误的唯一选择是死机，而这样它就不能再为攻击者所用。 而对于任意版本的IOS也不存在一个标准图像。每个图像都是建立在草图基础上，因此具体布局不仅受到版本的影响，还取决于编译的人员。就互操作性而言，这可能会导致一些问题，因为互操作性提倡设备的整体升级，尽管如此，它却为攻击带来了诸多不便。攻击者要想找到一个合适的地址来攻击都不是一件容易的事情。 所以，大多数路由开发都涉及配置事宜以及内部攻击。但是，这种情况可能会随着研究的深入而改变。其他IOS图像的分析师能够识别式样，从而可以很容易地找到目标地址。但是想保持路由运行并执行开发可不是一件简

单的事情。 好与坏，取决于你看事物的观点，对于一些新的服务，如VoIP，都是如此。VoIP可以在路由上生成更多客户型攻击面。 对路由器最好的保护是将网络设备中，或者是单独架构中的类似服务保持关闭状态，而且要确保只有管理者才有权操作路由器。 