基于Windows绕过文件限制和网络检测Microsoft认证考试 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_9F_BA_E4_BA_8EWind_c100_644598.htm 在2010年波士顿SOURCE大会上，安全研究人员表示，微软Windows的向后兼容性使攻击者能够绕过文件限制或网络安全防御（如入侵检测系统）。 核心安全技术公司的技术支持工程师Dan Crowley，介绍了几种在Web服务器（Nginx、Cherokee、Mongoose和LightTPD）的Windows版本中绕过这些保护的方法。最明显的是在Windows 中使用8.3别名。这些别名是兼容DOS的别名，它们在Windows创建一个文件时创建。这两个文件名都可以被访问，尽管它们不一样。 核心安全技术公司在今年二月报告了8.3文件系统别名漏洞。 8.3别名是8个字符的文件名，还有3个字符的文件扩展名。在Windows中，它们是文件名的前6个字符，后面是一个波形符、一个数字、一个点和文件扩展名（如~1.txt）。在文件名中所有其他字符被Windows截断。Crowley说，这大大增加了暴力攻击的效率，因为猜测文件名所需的时间和资源大大减少了。理论上，攻击者可以通过别名来调用文件，查看源代码，通过上传恶意软件操纵它。文件在下一次被合法调用时，系统就拥有了它。 他补充说，他的所有测试都是在基于Web的平台上完成的，但他表示，任何接受用户输入的应用程序都容易受到这种攻击。 Crowley说，“ 应用程序进行基于字符串的文件路径分析，这样做是为了决定如何处理文件、拒绝访问或确定恶意输入。这些替代文件名，甚至重整文件名，可以绕过或破坏很多东西。操作系统与文件系统交互，而不是应用程序。正因为如此，它

进行基于字符串的分析，将分析传到文件系统，如果它认为合法，就不需要文件系统确认了。”由IDS规则引起的问题，例如，如果他们寻找example.php，exampl~1就不会被标记。这样攻击者就能访问文件或发送远程代码。 Crowley说，一个缓解方法是禁用8.3别名。 他说，理想情况下，最好的缓解方法是停止基于字符串的文件路径分析。 编辑特别推荐: 略施小计Windows7资源管理器忘记历史 Windows7的安全小帮手MSE1.0 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com