Windows新的URI漏洞再现比前更危险 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/277/2021_2022_Windows_E6_96_B0_c100_277311.htm Mozilla的漏洞刚刚结束，微软的又来了，而且更加危险。Windows操作系统中的一个并不常用的功能可以导致严重的网络威胁。 安全研究者Billy Rios和Nathan McFeters说他们已经发现一个新的方法可以从受害者的计算机中窃取数据，方法就是利用Windows的浏览器通过URI（Uniform Resource IdentifIEr，统一资源标识符）引导应用程序这个过程中的漏洞。 在过去几个月里，自从Thor Larholm展示了如何使用URI技术欺骗IE浏览器发送恶意数据给Firefox以来，URI bug就已经成了热门话题，该漏洞允许攻击者在用户的PC上运行任意软件程序。还没过去多久，现在Rios和McFetters就展示了如何欺骗其他的浏览器和应用程序以达到类似的目标，目前的结果已经显示有很多种途径可以达攻击目的。 （利用此漏洞）可以通过URI来窃取用户计算机中的数据并远程上传内容给受害者。身为高级安全顾问的MvFetters说，这完全是通过应用程序提供的功能。 Shavlik的首席安全师Eric Schultze说：这是黑客的美梦成真，而程序员则噩梦到来，在随后几个月里攻击者们会找到多种多样的方法使正常的程序做出不正常的事情来。 通过使用自定义的URI协议名称，软件开发者们可以使用户更加方便地使用软件。Windows注册表会跟踪这些名称并将其分配给相关程序，这样任何时刻用户都可以通过浏览器调用相关程序。 例如AOL的即时信息客户端使用了aim的名称，因此点击那些以aim:goim开头的链接，或者在浏览器地址栏中输入aim:goim

，都会启动AIM即时消息窗口。 问题在于软件开发者们忙着启动程序，却并未考虑到收到的数据可能来自攻击者。 URI的处理问题相当复杂，甚至对与软件开发者来说也是如此。Mozilla最初以为Larholm的漏洞需要IE浏览器才能触发，但后来发现并非如此，随后的两周Firefox团队才补上这个漏洞。如果像Mozilla这样的组织在理解URI的处理过程中都会遇到问题的话，更不用说那些小规模的开发团队了。 