微软信息安全公告ActiveX漏洞最严重 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/269/2021_2022__E5_BE_AE_E8_BD_AF_E4_BF_A1_E6_c67_269290.htm Microsoft Agent ActiveX 控件中的漏洞 赛门铁克安全响应中心将Microsoft Agent ActiveX中的远程代码执行漏洞列为本月安全性公告中影响最严重的漏洞，由于ActiveX控件运行在大量的系统上，使用Microsoft Windows 2000操作系统的个人和企业用户如果访问一个恶意网页，就极易被利用。一旦成功利用，攻击者便可自行安装恶意代码，并有可能完全掌控受感染的系统。赛门铁克安全响应中心高级研究经理Ben Greenbaum表示：“赛门铁克今年观察到ActiveX漏洞明显增加。攻击者以人们所信赖的网络品牌为目标，如一些社会网络站点，然后等待受害者上钩，使其能够利用这一漏洞并进入受害者的电脑系统。由于存在‘概念证明性’公共代码，所以我们还认为MSN Messenger 和 Windows Live Messenger的漏洞是一个亟待解决的问题。”赛门铁克建议系统管理员采取以下措施： 评估这些漏洞对关键系统可能造成的影响。 规划必要的响应措施，包括采取适当的安全及可用性解决方案来部署更新修补程序，及执行最佳安全实践准则。 采取主动措施以保护网络和信息的完整性。 确认企业拥有合适及有效的数据备份流程和安全措施。 提醒用户谨慎打开所有来路不明的电子邮件附件，或链接来路不明/未经核实的网站。 赛门铁克建议家庭用户采取以下措施： 定期执行Windows Update，并且安装最新的安全性更新程序，以保持软件处于最更新状态。 不要打开来路不明的电子邮件附件，或链接来路不明/未经核实的网站。 使用

互联网安全方案如诺顿网络安全特警2007或诺顿360，以应对当今已知威胁，防护明日互联网安全风险。 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