

3 January 2007

By: Marius Oiaga, Technology News Editor

## [Highly Critical PDF Vulnerability](#)

*A patch is not yet available*



Symantec is expecting to see an escalation in online attacks via malicious PDF files, as it has reported a vulnerability related to Adobe Acrobat files and Cross Site Scripting. Hon Lau, a Sr. Security Response Engineer with Symantec has revealed that the Cupertino based security company has received reports of what he refers to as a "significant problem" that can result in the Adobe reader plugin executing malicious JavaScript code on the client side. "This stems from the "Open Parameters" feature in Adobe Reader, which allows for parameters to be sent to the program when opening a .pdf file. Like most things in life, this was a feature designed for benign usage, but unfortunately somebody has discovered that it can be used for malicious purposes also," said Lau. The reason why Symantec felt the need to ring the alarm is based on the fact that a successful attack via this vulnerability does not involve an exploit of flaws on the server side. "Any Web site that hosts a .pdf file can be used to conduct this attack. All the attacker has to do is find out who is hosting a .pdf file on their Web server and then piggy back on it to mount an attack using this method. What this means in a nutshell is that anybody hosting a PDF, including well trusted brands and names on the Web, could have their trust abused and become unwilling partners in crime," explained Lau. Adobe Systems has yet to release an official comment on the matter at hand, or a security patch addressing the issue. At the time of this article, the details surrounding the vulnerability are scarce to say the least. Symantec does not reveal if all versions of the Adobe Acrobat application are vulnerable or if any of the browsers available on the market manage to stop the execution of malicious JavaScript code. "To mitigate against attacks using this method you can implement JavaScript filtering capabilities to corporate firewalls and intrusion detection systems, and by disabling Adobe Reader plugin capabilities in Web browsers. As well as that, beware of people sending you links to .pdf files on the web. This would apply to all the usual distribution channels such as email, instant messaging, Web browsing, and so on. If you come across such a URL, look out for any unusual text or parameters after the .pdf extension," advised Lau.