

29 April 2009

By: Lucian Constantin, Web News Editor

[Two 0-Day Highly Critical Adobe Reader Vulnerabilities Disclosed](#)

They allow for remote code execution through malformed PDF files



Adobe Reader and Acrobat plagued by remote code execution flaws again
Adobe, Inc.

A hacker calling himself Arr1val has published proof-of-concept exploit codes for two 0-day vulnerabilities affecting Adobe Reader and Acrobat. The company has already confirmed one of them and strongly suggests disabling JavaScript in the products until a patch will be made available.

The flaws are classified by SecurityFocus as "boundary condition errors." The first is located in the [getAnnots\(\)](#) JavaScript function and the other in [spell.customDictionaryOpen\(\)](#). Both of them make it possible for an attacker to execute arbitrary code on systems with the affected products installed, by tricking users into opening a maliciously crafted PDF file.

According to Arr1val's PoC exploits, published on Packet Storm during the early hours of Tuesday, the vulnerabilities were tested on Adobe Reader 9.1 and Adobe 8.1.4 running on Linux. Adobe acknowledged the report and started an investigation into the issues. "We are currently investigating, and will have an update once we get more information," David Lenoe initially [announced](#) on the blog of Adobe's Product Security Incident Response Team (PSIRT).

He later returned with an update, [confirming](#) the [getAnnots\(\)](#) flaw in all Adobe Reader and Acrobat versions for all supported platforms, Windows, Mac and Unix. "We are working on a development schedule for these updates and will post a timeline as soon as possible," he pointed out. Meanwhile, disabling JavaScript entirely seems to be a way to mitigate possible attacks. This can be done by going to Edit -> Preferences -> JavaScript and unchecking the 'Enable JavaScript' option.

The company is still investigating the [spell.customDictionaryOpen\(\)](#) issue and is working with vendors in the AV and IT security industry to ensure that detection for these exploits is deployed to consumer products as quickly as possible. Vulnerability intelligence company Secunia [rates](#) the two vulnerabilities as "highly critical," its second highest-risk rating, and advises users not to open untrusted PDF documents, especially the people who need the JavaScript functionality.

Even though no attacks targeting these flaws have yet been reported in the wild, now that exploit code is available, that is very likely to change. And as past examples stand to show, it might take Adobe a considerable amount of time to release a fix. Back in February, when a similar 0-day critical [vulnerability](#) started being exploited in the wild, it took the company over three weeks to issue a patch.