

8 November 2008

By: Lucian Constantin, Web News Editor



Malicious PDF files exploit Adobe Reader and Acrobat vulnerability
Adobe Systems Inc.

[Recently Patched Adobe Reader Critical Flaw Targeted by Hackers](#)

Malicious PDFs that exploit the remote code execution vulnerability were detected in the wild

Bojan Zdrnja from the Internet Storm Center (ISC) warns that he has encountered [malicious PDF files](#), which exploit the recently announced and patched JavaScript-based buffer overflow vulnerability in Adobe Reader and Acrobat 8.1.2 and older. The attack is based on proof of concept code that was released on exploit tracking website Milw0rm soon after the vulnerability was disclosed.

As we reported a few days ago, Adobe has released an advisory and patches for several [serious flaws](#) detected in its Reader and Acrobat products. Five of the eight announced vulnerabilities allowed local and remote code execution, if exploited successfully. Only 8.1.2 and older versions of Adobe Reader and Acrobat were affected, but these versions are still in use on many systems, even though version 9 has been out for quite some time.

The vulnerability exploited by the malicious PDF file circulating on the Internet is identified as [CVE-2008-2992](#), and is probably the most serious of all. It was discovered by Damian Frizza from the CORE IMPACT Exploit Writers Team at Core Security Technologies, and it consists of a buffer overflow flaw in the way Adobe Reader handles the util.printf() JavaScript function.

The Core Security researcher demonstrated how an attacker could craft a malicious string argument that, when passed through this JavaScript function, allowed him to execute arbitrary code. Based on the [technical details](#) that Mr. Frizza disclosed, penetration tester and vulnerability researcher Debasis Mohanty created a [PoC exploit](#), which was posted on Milw0rm.

According to ISCs Bojan Zdrnja, the attackers that created the PDF files seen in the wild used Mohanty's proof of concept code, but made small changes like in the way the malicious string was being generated. As Zdrnja points out, unfortunately, this was enough to evade the detection mechanisms of anti-virus products, as none of the major 32 such products blocked or warned about the PDF file when it was scanned via the [VirusTotal](#) service.

Once opened, the malicious PDF files will call the legit mshta.exe Windows component in order to open remotely hosted .HTA (HTML Application) files. When executing these .HTA files, a Trojan application will be downloaded and installed on the target system. Mr. Zdrnja told [The Register](#) that the PDF files were served through rogue advertisements (malvertisements) that appear on suspicious websites.

Even though these files are currently spreading at a slow pace, the Internet Storm Center analyst speculates that the distribution rate will increase in the future, or that more attacks will be devised by other cybercriminals. Because of this, the users of the affected versions are highly encouraged to deploy the Adobe patch ([Windows](#), [Linux/Solaris](#), [Mac](#)) or to upgrade to [version 9](#) of Adobe Reader.