Discover two important zero-day vulnerabilities in Foxit PDF Reader

If you are using Foxit's PDF reader software, please carefully review it before being attacked.

Security researchers have discovered two very serious zero-day security holes in Foxit Reader software, which could allow hackers to execute random code on a target computer if not configured to open. file with Safe Reading Mode.

The first vulnerability **(CVE-2017-10951)** is a Bug Command Injection discovered by researcher Ariele Caltabiano, working at Trend Micro's Zero Day Initiative (ZDI). The second vulnerability **(CVE-2017-10952)** is a File Write discovered by researcher Steven Seeley at Offensive Security.

An attacker could exploit these vulnerabilities by sending a separate PDF file and forcing them to open them. Foxit refused to patch both of these vulnerabilities because they did not affect the Safe Reading Mode, which is enabled by default on Foxit Reader.

Foxit Reader & PhantomPDF has the Safe Reading Mode enabled by default, which controls JavaScript running. It can protect against unauthenticated JavaScript activities, 'the company said.

However, the researchers say that mitigation does not completely fix the gap. If it is not patched, it can be exploited if an attacker finds a way to bypass the Safe Safe Mode in the future.

Both unpatched vulnerabilities can be invoked via the JavaScript API on Foxit Reader.

1. **CVE-2017-10951:** Bug Command Injection is located on the app.launchURL function that executes the string that the attacker provides on the target system due to lack of proper authentication, described in the video below.

1. **CVE-2017-10952:** The vulnerability on the JavaScript saveAs function allows an attacker to write a random file on the target system at any of these addresses, described in the video below.

'Steven exploited this vulnerability by embedding the HTA file into a text file, then calling saveAs to write it on the startup directory, then executing the random VBScript code,' ZDI reports.

If you're using Foxit Reader or PhantomPDF, make sure you're turning on Safe Reading Mode. Alternatively, you can uncheck Enable JavaScript Actions on Foxit's Preferences section, although this may affect some features. Users are also encouraged to stay alert when opening any file received by email.