Foxit Reader bug lets attackers run malicious code via PDFs

Foxit Software, the company behind the highly popular Foxit Reader, has published security updates to fix a high severity remote code execution (RCE) vulnerability affecting the PDF reader.

This security flaw could allow attackers to run malicious code on users' Windows computers and, potentially, take over control

Foxit claims to have more than 650 million users from 200 countries, with its software currently being used by over 100,000 customers.

The company's extensive enterprise customer list contains multiple high-profile tech companies, including Google, Intel, NASDAQ, Chevron, British Airways, Dell, HP, Lenovo, and Asus.

Use after free weakness exposes users to RCE attacks

The high-severity vulnerability (tracked a CVE-2021-21822) results from a Use After Free bug found by Aleksandar Nikolic of Cisco Talos in the V8 JavaScript engine used by Foxit Reader to display dynamic forms and interactive document elements

Successful exploitation of use after free bugs can lead to unexpected results ranging from program crashes and data corruption to the execution of arbitrary code on computers running the vulnerable software.

This security flaw is caused by how the Foxit Reader application and browser extensions handle certain annotation types, which attackers can abuse to craft malicious PDFs that will allow them to run arbitrary code via precise memory control.

"A specially crafted PDF document can trigger the reuse of previously free memory, which can lead to arbitrary code execution," Nikolic explained.

"An attacker needs to trick the user into opening a malicious file or site to trigger this vulnerability if the browser plugin extension is enabled."

The vulnerability impacts Foxit Reader 10.1.3.37598 and earlier versions, and it was addressed with the release of Foxit Reader 10.1.4.37651.

To defend against CVE-2021-21822 attacks, you have to download the latest Foxit Reader version and then click on "Check for Updates" in the app's “Help” dialog.

More vulnerabilities fixed in Foxit Reader 10.1.4

Foxit fixed several other security bugs impacting previous Foxit Reader versions in the latest release, exposing users' devices to denial of service, remote code execution, information disclosure, SQL injection, DLL hijacking, and other vulnerabilities.

Understanding Security Vulnerabilities in PDFs

As more and more people talk about data breaches and computer security, the PDF reader is bound to come up. That’s because over the years, criminals have used files as a way to break into computers and networks. Unfortunately, whenever the news mentions a specific software or threat, people begin to worry about the safety and security of their organization’s assets. PDF files and the PDF reader are no exception, however, when you understand how these attacks work and what you can do to prevent them, you’ll feel more confident in your ability to minimize them.

Protecting your business software against security vulnerabilities

All types of software, your PDF reader needs to be updated when patches or new versions are released. That’s because these updates typically contain the code to fix zero-day vulnerabilities—the name given by security experts to vulnerabilities found and exploited by hackers that the vendor and security industry doesn’t know about—along with any other issues that developers may have found in the software.

You should also stay aware of any security vulnerabilities that are found in the software they rely on for day-to-day operations. Foxit makes these known to their customers through a security bulletins page in the support section of the Website

Understanding software security

Every type of software application is susceptible to vulnerabilities, not just PDF readers. Like every other type of software, PDF software undergoes extensive testing to plug any security holes. If a security vulnerability in a specific PDF reader is found, this doesn't mean that it will affect software created by other vendors. Exploits are usually application specific.

As long as organizations have something that others want, security will be a concern. Smart organizations do everything they can to fight back against these attackers—from educating staff about how to spot suspicious emails to making sure that their tools are up to date and patched. Working with vendors, especially when it comes to PDF readers, who take the security of their products seriously lays the foundation needed to keep your business safer.

The recommendations for users are quite simple and include:

- Foxit files and add-ons can be updated in several ways. Some updates are available if you open a.PDF document that triggers the updating process. For example, if you open a file that contains. Chinese characters, Foxit Reader will ask if you want to download the Eastern Asian Language. Support. Other updates are available only from the Help tab, where you have to manually install them. However, all updates can be downloaded directly from Foxit website.
- Security Warning Dialog – will warn users if a PDF document attempts to call or run an external command. The security warning dialog message provides a choice to run or terminate executing any files within a PDF file.
- Trust Manager (Safe Mode) – prevents suspicious external commands to be executed by Foxit Reader. The Trust Manager feature is easy-to-use and can be selected or deselected within Foxit Reader at the discretion of the user.
- Enhance Security with ASLR & DEP Support – increase security by making it harder for hackers to compromise a PDF document.

References:

- https://www.bleepingcomputer.com/news/security/foxit-reader-bug-lets-attackers-run-malicious-code-via-pdfs/?&web_view=true
- https://www.cybersafe.news/foxit-reader-bug-lets-attackers-run-malicious-code-via-pdfs/
- https://www.askwoody.com/forums/topic/foxit-reader-bug-lets-attackers-run-malicious-code-via-pdfs/
- https://www.haktechs.com/latest-hacking-news/malware-updates/foxit-reader-bug-lets-attackers-run-malicious-code-via-pdfs/
- https://www.foxitsoftware.com/blog/understanding-security-vulnerabilities-in-pdfs/
- https://www.foxitsoftware.com/blog/keep-yourself-safe-from-malicious-viruses/