LabVIEW vulnerability allows hackers to attack your computer

If you need to use LabVIEW software to design machines or industrial devices, you should be alert when opening any VI file (virtual instrument). Recently, security researchers have discovered a serious flaw in this software.

If you need to use LabVIEW software to design machines or industrial devices, you should be alert when opening any VI file (virtual instrument).

LabVIEW is developed by the US company - National Instruments - is a visual programming language and a powerful system design tool used worldwide in hundreds of areas. In addition, it provides engineers with a simple environment to build measurement or control systems.

Recently, Cisco Talos Security Intelligence security researchers have discovered a serious flaw in this LabVIEW software. This vulnerability allows an attacker to execute malicious code on the destination computer and control the entire system.

1. How to protect high-risk network ports?
2. EternalRocks - more dangerous malicious code than WannaCry exploits up to seven NSA vulnerabilities

Defined as CVE-2017-2779, this executable code vulnerability can be activated by opening a special VI file - a file format that LabVIEW uses. This vulnerability stems from memory errors in the RSRC segment parsing function of LabVIEW.

Talos researchers explained that: *A specially created LabVIEW VI file (with * .vi extension) can help an attacker control loop status and write nulls at will* .

Researchers have also successfully tested the vulnerability in LabVIEW 2016 version 16.0 but National Instruments does not recognize this as a flaw and does not release a patch for this vulnerability.

Because there is no patch available, LabVIEW users have only one option to be careful when opening any VI file received via email.