Detecting zero-day vulnerability in the Dropbox 10 Windows app, users pay attention!

A group of free security researchers recently announced the zero-day vulnerability in the Dropbox version of the Windows app.

A group of freelance security researchers recently announced a zero-day vulnerability in the Windows-based Dropbox app, which could allow an attacker to gain extremely simple SYSTEM privileges.

Specifically, two free security researchers, nicknamed Chris Danieli and Decoder, discovered the vulnerability for the first time in early September and informed Dropbox of the vulnerability on September 18. At that time, Dropbox pledged to take remedies within 90 days. However, more than 3 months have passed, Dropbox has not been able to release a security patch for this vulnerability, so Chris Danieli and Decoder decided to issue a public notice to warn users.

The flaw exists in the Windows Dropbox application and is an arbitrary file overwriting problem, which can give an attacker access to local user escalation to execute remote code as SYSTEM. According to the researchers, the problem most likely originated in the DropboxUpdater service.

DropboxUpdater is installed as part of the Dropbox client software, and the team says it runs as SYSTEM in standard installations as well as "one of the dropboxupdate tasks is run hourly by the task scheduler. (task scheduler) ". Once activated, the system will record a log file and send to the location of the SYSTEM account - this is the point that allows hackers to 'take action'. Indeed, the researchers successfully overwrote the files controlled by the SYSTEM account and took hold of the shell, the command-line interface with those SYSTEM privileges.

Fortunately, it is not easy for hackers to exploit this vulnerability. First and foremost, an attacker must possess local user access to the target computer, which means that the hacker 's accessibility has been significantly

reduced. But not so that you are allowed to be subjective. The Dropbox application needs to be installed in a standard way, complete with administrator privileges, but since most people leave it as default, the risk remains.

As reported by Bleeping Computer experts, a "micro-patch" currently available on oPatch can temporarily fix this problem (by cutting the logging code from DropboxUpdater) until the 'genuine' fix. 'from Dropbox is launched.

As for Dropbox, a company spokesman said: 'We have learned about this issue through the bug bounty program and will offer a fix in the coming weeks. This vulnerability can only be exploited for limited use and we have not received any reports of it affecting our users. '