Critical error on Skype allows hackers to execute malicious code remotely

A serious flaw was discovered on Microsoft's chat and call application, allowing hackers to remotely execute malicious code and cause system crashes.

Skype is a popular messaging application that allows users to chat online, make video calls via the Internet, and support multiple platforms. Microsoft acquired Skype from May 2011 for $ 8.5 billion due to its global popularity.

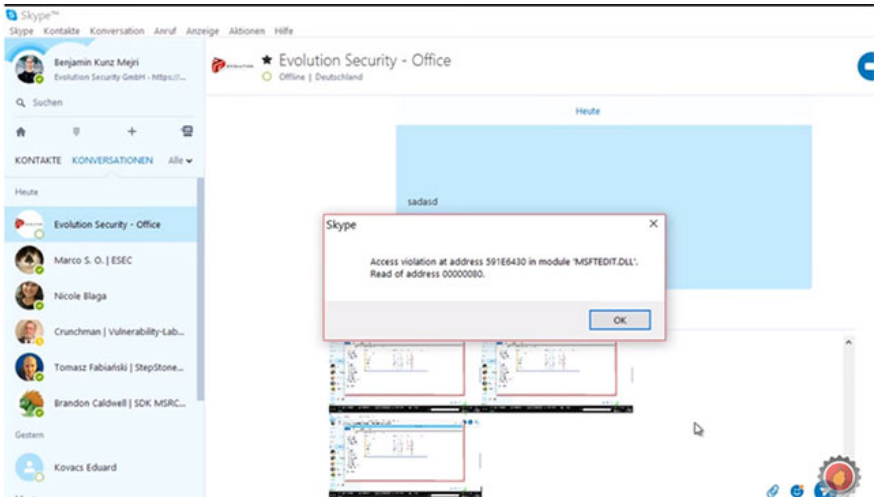
Network security researcher Benjamin Kunz-Mejri from the German organization Vulnerability Lab discovered a buffer overflow that was previously unknown, called **CVE-2017-9948,** on the Skype version of the application. web during group call. This vulnerability is said to have a high level of risk with a score of 7.2 CVSS and affect Skype version 7.2, 7.35 and 7.36 on Windows XP, Windows 7 and Windows 8, Mejri said in a public release document. on Monday.

> 'This problem can be exploited remotely via local session or interaction. The problem identified on the clipboard or cache is transferred via remote session on Windows XP, Windows 7, Windows 8 and Windows 10. This vulnerability on Skype version 7.37 has been patched. '

Users do not need to interact

What's the worst thing? Buffer overflow errors do not require user interaction and only a low level of Skype user accounts. Therefore, an attacker can crash a remote application 'with an unexpected error to override the process registration' or even execute the malicious code on a system running vulnerable versions of Skype.

This error is in the way Skype uses the **MSFTEDIT.DLL** file in case it needs to copy the request on the system.



Hackers can execute malicious code remotely on victim machines via Skype

How do attackers exploit vulnerabilities?

According to the report, an attacker will create a tainted image file, copy and paste from the computer clipboard to the Skype user's chat window. When the file is located on the clipboard of both local and remote systems, Skype will be overflowed by buffer, causing errors and application crashes, open to hackers to exploit.

" The limit of file size through the session with the remote clipboard has no safety limit. An attacker could crash the software with a request to override the EIP subscription of the active software process, 'said Vulnerability Lab. 'Therefore, it allows local and remote attackers to execute their code on connected and infected computers via Skype'.

PoC code

The company also provides a PoC exploit code that you can use for testing. The Vulnerability Lab reported bugs to Microsoft on May 16, and Microsoft fixed the bug, released a patch on June 8 for Skype version 7.37.178. If you're using Skype, make sure you install the latest version to protect yourself.