Discovered a particularly dangerous vulnerability in Cisco Jabber video conferencing software

If the vulnerability in Cisco Jabber is exploited successfully, the hacker will gain control of the victim's computer.

Network equipment maker Cisco has released a new version of its Jabber web conferencing and messaging application for Windows 10. This new release includes fixes for many of the vulnerabilities that, if exploited, can expose them. allow hackers to attack, install and run arbitrary software on the victim's machine.

The vulnerabilities, discovered by Norwegian cybersecurity firm Watchcom, affect all active versions of Cisco Jabber. And for now, they have been patched by Cisco.

Two of the four vulnerabilities can be exploited to install and run arbitrary software on a victim's machine by sending messages specifically designed for group or individual chats.

The most serious of these was the codenamed CVE-2020-3495 vulnerability, a CVSS hazard rating of 9.9. This vulnerability leads to incorrect message content validation, so hackers can use them to send messages designed according to Extensible Messaging and Presence Protocol (XMPP).

"When the exploit is successful, the hacker can cause the application to launch arbitrary programs on the victim's system with the privileges of the user account running Cisco Jabber. From there, the hacker can run any code. or any software, " Cisco revealed.

Just a few days ago, Cisco had to warn of a zero-day vulnerability being actively exploited by hackers in the software of the IOS XR router.

Cisco recommends that users update to the latest version of Jabber software immediately.