Serious flaw allows Cisco IP phones to be used for spying

Researchers have demonstrated how a serious vulnerability in the 7900 series of the Cisco (NASDAQ: CSCO) Unified IP Phones can be used to transform them into bugging devices in order to eavesdrop on private conversations.

This is possible due to a flaw that allows part of the phone's memory to be rewritten, thereby allowing an attacker to gain root access and remotely switch on the phone's microphone from literally anywhere in the world. The flaw was discovered by doctoral candidate Ang Cui and Columbia University Professor Sal Stolfo, who say that it may also cause phones' web cameras to turn on.

Cisco said in response that "all Cisco IP phones feature a hard-wired light that will alert the user whenever the microphone is active." The company is also working on a permanent patch to the flaw with its "A-Team."

However, the researchers were able to demonstrate the speaker LED light remaining dark even with the microphone enabled. "There is no hard-wired light," Cui was reported as saying. "Everything is controlled by the software."

The problem is worrisome given the large number of enterprises and government organizations that may be using Cisco phones. Though it can be argued that best practices dictate that IP-based phones are located on their own networks, this may not be the case in many organizations. Moreover, the researchers have shown that a hacked phone can be used to corrupt other phones on the network.

For now, Cisco is suggesting that administrators restrict SSH and CLI access to trusted users only. In addition, administrators may also want to use 802.1x device authentication to prevent unauthorized devices or systems from accessing the network.