Issued 2/15/18

Skype Can't Fix a Nasty Security Bug without a Massive Code Rewrite

A security flaw in Skype's updater process can allow an attacker to gain system-level privileges to a vulnerable computer. The bug, if exploited, can escalate a local unprivileged user to the full "system" level rights -- granting them access to every corner of the operating system. But Microsoft, which owns the voice- and video-calling service, said it won't immediately fix the flaw, because the bug would require too much work. Security researcher Stefan Kanthak found that the Skype update installer could be exploited with a DLL hijacking technique, which allows an attacker to trick an application into drawing malicious code instead of the correct library. An attacker can download a malicious DLL into a user-accessible temporary folder and rename it to an existing DLL that can be modified by an unprivileged user, like UXTheme.dll. The bug works because the malicious DLL is found first when the app searches for the DLL it needs. Once installed, Skype uses its own built-in updater to keep the software up to date. When that updater runs, it uses another executable file to run the update, which is vulnerable to the hijacking. The attack reads on the clunky side, but Kanthak told ZDNet in an email that the attack could be easily weaponized. He explained, providing two command line examples, how a script or malware could remotely transfer a malicious DLL into that temporary folder. "Windows provides multiple ways to do it," he said. But DLL hijacking isn't limited to Windows, he said -- noting that it can apply to Macs and Linux, too. Once "system" privileges are gained, an attacker "can do anything,"

Kanthak said. From there, an attacker could steal files, delete data, or hold data hostage by running ransomware.