Microsoft attributes new SolarWinds attack to a Chinese hacker group



Microsoft's Threat Intelligence Center (MSTIC) reported on Tuesday that SolarWinds software was attacked with a zero-day exploit by a group of hackers it calls "DEV-0322." The hackers were focused on SolarWinds' Serv-U FTP software, with the presumed goal of accessing the company's clients in the US defense industry.

The zero-day attack was first spotted in a routine Microsoft 365 Defender scan. The software noticed an "anomalous malicious process" that Microsoft explains in more detail in its blog, but it seems the hackers were attempting to make themselves Serv-U administrators, among other suspicious activity.

Update Serv-U as soon as possible

SolarWinds reported the zero-day exploit on Friday, July 9th, explaining that all of the Serv-U releases from May 5th and earlier contained the vulnerability. The company released a

hotfix to address the issue and the exploit has since been patched, but Microsoft writes that if Serv-U's Secure Shell (SSH) protocol connected to the internet, the hackers could "remotely run arbitrary code with privileges, allowing them to perform actions like install and run malicious payloads, or view and change data." Anyone running older Serv-U software is encouraged to update it as soon as possible.

The first hack that shoved SolarWinds into the limelight in December 2020 exposed hundreds of government agencies and businesses. Unlike the previous hack, which is now widely connected to a Russian state-affiliated group of hackers called Cozy Bear, Microsoft says this zero-day attack originated in China. DEV-0322 has made a habit of attacking "entities in the US Defense Industrial Base Sector," Microsoft writes, and is known for "using commercial VPN solutions and compromised consumer routers in their attacker infrastructure."

https://www.theverge.com/2021/7/14/22577471/microsoft-solarwinds-hack-zero-day-serv-u