UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00135

ZOOM RCE ZERO-DAY ATTACK CHAIN

DATE ISSUED: 19th April 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Computest researchers have recently discovered a zero-day 3-step attack chain whilst in the popular video conferencing software Zoom that allows Remote Code Execution without any interaction from the user.

BREAKDOWN

While competing in the recent Pwn2Own contest, the Computest entrants demonstrated the ability to open the calculator application of a device remotely that was running Zoom following the exploit of the bug-chain. The attack was demonstrated in Windows and Mac devices with a local installation of the software, and it is not yet known if it will affect iOS and Android devices as well. The browser version seems to be unaffected as well as in-session Zoom meetings and Zoom video webinars. Specific technical details are being kept under wraps as Zoom attempts to develop a fix. The attack was carried out under the scenario that the attacker must belong to the same organizational account or be an accepted external contact to carry out the attack.

REMEDIATION STEPS

- Stay up to date on communications from Zoom regarding the availability of security patches – standards allow a 90-day window for vendors to issue patches.
- Install software updates for Zoom when prompted but ensure they are legitimate before installation.
- Ensure you are running the latest version of Zoom for desktop.

REFERENCES & RESOURCES

ZDNet	https://www.zdnet.com/article/critical-zoom-vulnerability-triggers-remote-code-execution-without-user-input/
Malwarebytes	https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/04/zoom-zero-day-discovery-makes-calls-safer-hackers-200000-richer/
Zoom	https://support.zoom.us/hc/en-us/articles/201362233-Upgrade-update-to-the-latest-version
Tom's Guide	https://www.tomsguide.com/uk/news/zoom-security-flaw-pwn2own