- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Vulnerabilities

Details Disclosed for Zoom Exploit That Earned Researchers $200,000

By Eduard Kovacs on August 24, 2021

Researchers have disclosed the details of a Zoom exploit that could have allowed malicious actors to achieve remote code execution without user interaction.

The exploit was demonstrated on April 7 at the 2021 Pwn2Own hacking competition by Daan Keuper and Thijs Alkemade from Computest. The researchers earned $200,000 for demonstrating that the exploit could be used to remotely execute arbitrary code on the targeted system.

Exploits demonstrated at Pwn2Own are reported to the vendors and Zoom immediately started working on a patch. According to an advisory published by Zoom on August 13, the most severe of the flaws leveraged in the exploit chain used by Keuper and Alkemade, tracked as CVE-2021-34407, was patched in the Zoom Client for Meetings version 5.6.3, which the company released on April 19. In addition, a server-side fix was implemented just a few days after Pwn2Own.

The Zero Day Initiative (ZDI), which organizes Pwn2Own, on August 17 made public advisories for each of the three vulnerabilities chained at the contest to hack Zoom. In addition to CVE-2021-34407, which is a high-severity heap-based buffer overflow that allows remote code execution, the exploit chain involved a directory traversal bug related to the processing of GIPHY messages, and an information disclosure issue related to Zoom Marketplace URLs.

In order to trigger the exploit, the attacker would need to send a series of specially crafted messages to the targeted user. While the exploit would be triggered automatically — without the user clicking on anything — Zoom and the researchers noted that for the exploit to work, the targeted user needed to accept an external connection request or be in the same multi-user chat as the victim.

The Computest researchers on Monday published a technical write-up detailing the vulnerabilities and how they were discovered, in an effort to help others who might want to conduct similar research in the future.

“In total we spent around 1.5 weeks from the start of our research until we had the main vulnerability of our exploit,” they explained. “Writing and testing the exploit itself took another 1.5 months, including the time we needed to read up on all Windows internals we needed for our exploit.”

Related: Details Disclosed for Critical Vulnerability in Sophos Appliances

Related: Zoom Is 16th CVE Numbering Authority Appointed in 2021

Related: Zoom Patches Two Serious Vulnerabilities Found by Cisco Researchers

Related: Zoom Working on Patch for Code Execution Vulnerability in Windows Client

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia’s security news reporter. Eduard holds a bachelor’s degree in industrial informatics and a master’s degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:
OpenSSL Vulnerability Can Be Exploited to Change Application Data
XDR Firm Hunters Raises $30 Million in Series B Funding
Details Disclosed for Zoom Exploit That Earned Researchers $200,000
T-Mobile Sued Over Data Breach Affecting Millions of Customers
Realtek SDK Vulnerabilities Exploited in Attacks Days After Disclosure

Tags:
NEWS & INDUSTRY Vulnerabilities

Search

Get the Daily Briefing

BRIEFING