SECURITYWEEK NETWORK:

- Cybersecurity News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2021 CISO Forum
- ICS Cyber Security Conference
- Contact

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance

- 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 › Endpoint Security

Zoom Patches High-Risk Flaws in Meeting Connector, Keybase Client

By Ryan Naraine on November 12, 2021

Video messaging technology giant Zoom has shipped patches for high-severity vulnerabilities that expose enterprise users to remote code execution and command injection attacks.

The company released multiple security bulletins to warn of the risks and called special attention to a pair of “high-risk” bugs affecting its on-prem meeting connector software and the popular Keybase Client.

“The network proxy page on the web portal for the [affected] products fails to validate input sent in requests to set the network proxy password. This could lead to remote command injection by a web portal administrator,” Zoom said in a note.

The CVE-2021-34417 carries a CVSS Base Score of 7.9, and affects multiple Zoom software components -- Zoom On-Premise Meeting Connector Controller, Zoom On-Premise Meeting Connector MMR, Zoom On-Premise Recording Connector, Zoom On-Premise Virtual Room Connector.

[READ: Vulnerability Allowed Attackers to Join Zoom Meetings]

A second high-severity bulletin was also released with patches for CVE-2021-34422, a path traversal bug affecting Keybase Client for Windows.

From Zoom's advisory:

> "The Keybase Client for Windows before version 5.7.0 contains a path traversal vulnerability when checking the name of a file uploaded to a team folder. A malicious user could upload a file to a shared folder with a specially crafted file name which could allow a user to execute an application which was not intended on their host machine."
>
> "If a malicious user leveraged this issue with the public folder sharing feature of the Keybase client, this could lead to remote code execution."

Zoom said the issue was fixed in the 5.7.0 Keybase Client for Windows release.

Zoom's security response team also shipped patches for a medium-risk bug (CVE-2021-34420) in the Zoom Client for Meetings installer. "The Zoom Client for Meetings for Windows installer before version 5.5.4 does not properly verify the signature of files with .msi, .ps1, and .bat extensions. This could lead to a malicious actor installing malicious software on a customer's computer," the company warned.

The Zoom software does not have an automatic update mechanism. Users are urged to manually check for software updates within the Zoom client.

Related: Remote Code Execution Flaw in Palo Alto GlobalProtect VPN

Related: Adobe Patches Critical RoboHelp Server Security Flaw

Related: Zero-Days Under Attack: Microsoft Plugs Exchange Server, Excel Holes

Ryan Naraine is Editor-at-Large at SecurityWeek and host of the popular Security Conversations podcast series. He is a journalist and cybersecurity strategist with more than 20 years experience covering IT security and technology trends. Ryan has built security engagement programs at major global brands, including Intel Corp., Bishop Fox and Kaspersky GReAT. He is a co-founder of Threatpost and the global SAS conference series. Ryan's career as a journalist includes bylines at major technology publications including Ziff Davis eWEEK, CBS Interactive's ZDNet, PCMag and PC World. Ryan is a director of the Security Tinkerers non-profit, and a regular speaker at security conferences around the world. **Follow Ryan on Twitter @ryanaraine.**

Previous Columns by Ryan Naraine: