Community Alert: New Critical ConnectWise Vulnerability Actively Exploited

Cybercriminals around the world are racing to exploit a new critical vulnerability that affects the popular ConnectWise ScreenConnect Remote Monitoring and Management (RMM) software, used by thousands of organizations and MSPs to remotely manage their technology environments. The devastating outage of Change Healthcare (part of Optum), which has disrupted prescription processing services for over 67,000 pharmacies and 129 million individuals, was traced back to exploitation of this new vulnerability.

The attack is very simple; hackers only need a web browser to exploit a target. EVERY ORGANIZATION SHOULD IMMEDIATELY ASSESS YOUR RISK AND DETERMINE IF KEY SUPPLIERS ARE AFFECTED. Already, hackers are actively leveraging these vulnerabilities to:

- **Gain full remote access to Internet-facing software and servers**
- **Steal data and other sensitive information**
- **Expand access to systems** throughout your network
- **Install additional malware, add accounts and place backdoors** in your network
- **Detonate ransomware** and hold your organization hostage.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued guidance urging all organizations to apply the updates immediately. See below for details.

What You Need to Do

- ✓ **Immediately check and determine whether you are running affected software.** This includes on-premise ScreenConnect versions 22.4 through 23.9.7, according to the ConnectWise announcement which can be found here: https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
- ✓ **Apply updates to any on-premise ScreenConnect servers to prevent exploitation.** The minimum version to prevent exploitation is version 23.9.8.
- ✓ **Restrict access to the ScreenConnect login interface**, if possible.
- ✓ **Conduct routine vulnerability scanning (ideally daily)** to ensure that the affected systems remain patched and up-to-date.
- ✓ **Routinely conduct penetration tests to ensure perimeter security and minimize the risk of lateral movement.**
- ✓ **Search affected systems for indicators of unauthorized access** or data exfiltration. If indicators of compromise are found, initiate your incident response procedures.
- ✓ **Carefully monitor and respond to all alerts** relating to affected devices.
- ✓ **Verify backups are working properly and can't be overwritten** in case ransomware hits.

Check Your Suppliers

Proactively reach out to key suppliers such as MSPs, software vendors and cloud providers to assess your risk and take action if needed.

- **Prioritize your suppliers based on their access to your sensitive data and/or network resources.** Identify suppliers that store or process sensitive data on your behalf or which have

a high degree of access to your IT resources and focus on following up with these organizations first.

- **Ask your suppliers to confirm whether they or any partners or service providers connected to their network use an affected version of ScreenConnect.** If so:
    - **Determine whether the supplier updated** to the latest version of ScreenConnect (minimum version 23.9.8), or if not, what their timeline is for updating.
    - **Evaluate the risk that your sensitive data and/or IT resources could have been impacted** due to the vulnerability.
- **Ask your suppliers if they are actively assessing risk due to *their* supply chain**, and if so, whether any evidence of compromise has been identified (fourth- and even fifth- party risks are real and have led to many data breaches and cybersecurity incidents).
- **Make sure to give your suppliers a deadline for responding** so that you can coordinate your own response and public relations efforts.

Stay Up-to-Date

LMG will continue to monitor the developing situation and provide updates as they become available. If you have any questions or need assistance with vulnerability scanning or securing your environment, please email info@LMGSecurity.com.

Email: info@LMGsecurity.com;

Phone: 406-830-3165