+44 345 094 0945
www.waterstons.com

Article

Oct 2024

Critical vulnerabilities in remote access tools expose industrial networks to cyber threats

Claroty's Team82 recently discovered a critical vulnerability in industrial networks: the widespread use of insecure remote access tools (RATs) in Industrial Control Systems (ICS) and Operational Technology (OT) environments.

Sean-Francis Brown
Senior Information Security Consultant
Email sean.brown@waterstons.com

Analysing 50,000 remote access-enabled devices, Team82 found that 55% had at least four RATs, while 33% had six or more. Some organisations even reported up to 16 different tools in use. Many of these tools lacked essential security features, such as multi-factor authentication (MFA) and session recording, leaving critical infrastructure sectors - including oil and gas, manufacturing, and healthcare - exposed to cyber threats.

These vulnerabilities have already been exploited in high-profile breaches like the Colonial Pipeline attack in 2021. Additionally, attackers are actively targeting these weaknesses, leveraging tools such as TeamViewer and AnyDesk to compromise ICS environments.

Wider context

This incident highlights the growing threat to ICS/OT environments, where the demand for remote access has rapidly expanded attack surfaces. The combination of tool sprawl and weak security controls has made ICS networks prime targets for attackers, especially in critical infrastructure sectors like energy, pharmaceuticals, and manufacturing.

The threat landscape for ICS/OT environments is shifting, with adversaries increasingly focusing on supply chain attacks and exploiting vulnerabilities in remote management tools.

Cybercriminals and nation-state actors alike are capitalising on these opportunities to infiltrate industrial networks, disrupt operations, or steal valuable data. Recent attacks show a clear trend: misconfigured or outdated RATs are becoming a preferred entry point for malware, ransomware, and cryptomining campaigns.

Recommendations

Inventory and monitor remote access tools: Organisations should conduct a comprehensive audit of all remote access tools in use across their ICS/OT environments. This will provide visibility into the number of tools and their security posture.

Eliminate insecure tools: Remove or replace RATs that do not meet basic enterprise security standards. Ensure all tools used are up-to-date and supported by vendors with regular security patches.

Enforce strong authentication: Implement multi-factor authentication (MFA) for all remote access connections, particularly those related to ICS/OT systems, to prevent unauthorized access.

Establish security baselines: Develop and enforce minimum security requirements for all remote access tools used within the organisation and across third-party supply chains, ensuring alignment with industry best practice

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430