CIAC
Colorado Information Analysis Center
Department of Public Safety

04 October 2024
24-0001298

CIAC CYBER UNIT

October 04, 2024

Summary: The CIAC has been made aware of suspicious activity targeting VPN clients on SCADA networks in Colorado. A critical infrastructure entity in the water sector has reported that a number of their accounts within their SCADA network became temporarily inaccessible due to a vulnerability that allowed access to a VPN Portal Login Page. This portal allowed attackers to conduct password attacks against accounts on the SCADA network. The entity disabled the portal after confirming that the necessary systems had the VPN clients installed.

Recommendation: Assess the necessity of maintaining web-accessible VPN portals, especially those exposed to the internet. Consider disabling any non-essential access points to reduce the risk of password-based attacks, which could compromise critical systems. Focus on minimizing access points to sensitive infrastructure and ensure strict controls are in place for any that remain.

At this point in time, organizations are encouraged to exhibit increased vigilance and follow best practices for detecting unauthorized activity such as monitoring firewall and EDR appliances for any unusual activity. Additionally, recipients of this message and organizations who are experiencing similar activity are encouraged to reach out to the CIAC Cyber Unit at cdps_ciac_cyber@state.co.us and share any pertinent information that could contribute to a more accurate understanding of the incident.