COMMONWEALTH OF PENNSYLVANIA
PENNSYLVANIA PUBLIC UTILITY COMMISSION
COMMONWEALTH KEYSTONE BUILDING
400 NORTH STREET
HARRISBURG, PENNSYLVANIA 17120

February 6, 2024

To All Jurisdictional Pennsylvania Public Utilities:

On January 31, 2024, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released a joint alert warning Small Offices and Home Offices (SOHO) about the potential dangers associated with using outdated or inexpensive routers. Routers are essential for connecting Information Technology (IT) devices (computers, phones, tablets, printers, etc.) to the internet, and they are responsible for sending and receiving signals from the Internet Service Provider (ISP) and dispersing the signal to devices on the network.

The Pennsylvania Utility Commission (PUC) is concerned that some of our smaller regulated utilities and utilities that have teleworkers may be using outdated or inexpensive SOHO routers to create Local Area Networks (LANs) to connect their IT devices to the Internet. We want to make you aware that security defects in older or inexpensive routers can be exploited by nation states and their proxies to use them to compromise other U.S. critical infrastructure entities.

The issue is that many of the SOHO routers are either no longer being supported by the manufacturer and no longer being updated; or are inexpensive and lack the necessary security features that more expensive routers provide. These vulnerabilities enable these threat actors to install malware onto these devices and use them to either conduct further attacks on the devices on the local area network or turn the devices into a covert messaging infrastructure for the threat actors to launch a cyber-attack on other critical infrastructure stakeholders. For more information about this issue, please reference the following information:

U.S. Department of Justice – Press Release: U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure

CISA Alert – Security Design Improvement for SOHO Device Manufacturers

CISA Cybersecurity Advisory – People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Lumen Blog – Routers Roasting on an Open Firewall: The KV-Botnet Investigation

To protect yourself, the Commission strongly urges utilities that use SOHO routers to contact their ISP to determine if their router is outdated and no longer receiving updates. If the router is outdated, request a new router with more up-to-date security functions. If you have IT support, you can also consult with them to ensure that they are using the most current routers and that they are secure. Finally, utilities with teleworkers who have home offices may also be susceptible to this threat, and you might want to make them aware of this threat as well.

Respectfully,

Michael Holko, Director, Office of Cybersecurity Compliance and Oversight
Pennsylvania Public Utility Commission
400 North Street, 3rd Floor North
Commonwealth Keystone Building, Harrisburg, PA 17120
717-425-5327 | miholko@pa.gov
www.puc.pa.gov |Consumer Hotline 1-800-692-7380
Follow us on: