Volt Typhoon: State-Sponsored Cyber Actor

Overview

On May 24, 2023, GE Gas Power was made aware of the Volt Typhoon state-sponsored actor based in China typically focused on espionage and information gathering. The group's campaign targets critical infrastructure providers and their tactics for achieving and maintaining unauthorized access to target networks.

Vulnerability Details

This group utilizes tactics, techniques, and procedures (TTP) to leverage on built-in network administration tools to evade detection by blending with normal Windows system, put data into an archive file to stage it for exfiltration, and use the stolen credentials to maintain presence. The group also avoids endpoint detection responses that would alert on the introduction of third-party applications to the host and limit the amount of activity that is captured in default logging configurations.

Exploitation Status

While the group tries to compromise network equipment such as, routers, firewalls, and VPN hardware, GE Gas Power performed a global inventory assessment to determine if there is a risk exposure to systems regarding the indicator of compromise (IOCs) and whether there is a significant risk exposure to GE Gas Power assets. Our findings indicate that no GE Gas Power assets are impacted by this vulnerability, and no Indicators of Compromise (IOCs) were detected during the assessment.

Contact Information

GE Gas Power is committed to ensuring the safety, security, integrity, and regulatory compliance of our products. Contact your local GE Services representative for assistance or for additional information.

For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Document History

Version	Release Date
1.0	6/27/2023