GE Gas Power

GE Gas Power Product Security Incident Response and Vulnerability Handling

WHITEPAPER

Introduction

GE Gas Power works continuously to provide highly secure products and services for its customers, but security incidents and vulnerabilities are an inevitable reality that must be thoroughly and swiftly managed. This paper provides an overview on how GE Gas Power handles security incidents, leveraging industry standard methods and technologies to minimize any potential impact. GE's primary goal when responding to security incidents is to protect the customer environment. GE also strives to protect the products and services our customers rely upon, and maintain the highest level of integrity in our products. The Gas Power Product Security team and the various service teams work jointly to manage any security incident and accomplish these goals.

Gas Power Security Incident Response Mechanism

GE Gas Power's approach to managing a security incident conforms to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61. We have a dedicated team that works to prevent, monitor, detect, and respond to security incidents across the Gas Power portfolio.

Incident and Vulnerability Monitoring

GE Gas Power Product Security continuously monitors different channels (internal and external) for security incidents and vulnerabilities information. All Gas Power employees receive annual training to recognize and report signs of potential security incidents, including phishing attacks, unauthorized devices, and cyber hygiene. Any suspicious activity detected by employees, customers, or security monitoring tools are escalated to Product Security Incident Response Team for investigation.

The Product Security also regularly assesses product security through internal and external assessments. These reviews look for vulnerabilities in third party libraries, checking for known attack vectors and ways to compromise the product. The results of these assessments are reported back to the product teams with mitigation recommendations, so they can be appropriately addressed.

Incident and Vulnerability Response Plan

Gas Power has developed and implemented a closed-loop security incident and vulnerability handling process that includes prevention, detection, correction and recovery, and post-incident feedback. Once a security incident occurs, the GE Gas Power quickly analyzes the incident and takes necessary measures to control the impact. After the incident is effectively controlled, review and improvement will be carried out to prevent the recurrence of similar incidents.

Product Security Incident Response Team (PSIRT)

We have established a PSIRT that is responsible for receiving, processing and disclosing security vulnerabilities on Gas Power products and solutions. When suspicious activity is detected and escalated, PSIRT will initiate a process of **analysis, containment, eradication, and recovery**. They conduct an analysis of the potential incident to determine its scope, including any impact to customers or customer data. Based on this analysis, PSIRT will work with relevant stakeholders to develop a plan to contain the threat and minimize the impact of the incident, eradicate the threat from the environment, and fully recover to a known secure state.

Test of Incident Response Capabilities and Processes

At Gas Power, we continually test and improve the processes created to communicate, collaborate, and restore services in the event of a cyber incident. We routinely evaluate our response capabilities against the current cyberthreat landscape, evolving and adapting as necessary to ensure the greatest level of protection for our customers.

Notification

Whenever Gas Power becomes aware of a Product Security Incident and Vulnerability, GE notifies affected its customers as quickly as possible. Notifications include a description of the nature of the security incident or vulnerability, approximate impact, and mitigation steps (if applicable). If GE's investigation isn't complete at the time of initial notification, the notification will also indicate next steps and timelines for subsequent communication.

If a customer becomes aware of an incident that could have an impact on Gas Power products and solutions, the customer should promptly notify GE of the incident, at which point we can partner to isolate and remedy the incident appropriately.

Private Sector and National Resource Engagement

Adhering to the principle of openness and transparency, Gas Power actively cooperates with security organizations and makes responsible disclosures of vulnerabilities discovered internally and externally by customers and related parties. For confirmed vulnerabilities, Gas Power provides mitigation measures and solutions, and monitors the result after the customer implements the solutions, so as to iterate solutions in a closed-loop manner.

Gas Power is one of the CVE Numbering Authorities (CNA) and has established and implemented a Coordinated Vulnerability Disclosure (CVD) program.

GEA35217 (10/2022)