NEWS RELEASE

Resonac Holdings Corporation
Tokyo Shiodome Bldg., 1-9-1, Higashi-Shimbashi
Minato-ku, Tokyo 105-7325

June 3, 2025

Regarding the Security Incident at Our Company (Fourth Report: 3:30 pm, June 3)

Resonac Holdings Corporation (hereinafter referred to as “our company”) previously announced the first report on May 20 and the third report on May 23 regarding a security incident that occurred at our company. Our emergency response headquarters has been investigating the scope of the impact and working diligently to restore systems and resume normal operations as quickly as possible.
We sincerely apologize for the great concern and inconvenience caused to our business partners and related parties.
While it will take some more time to fully understand the extent of the damage and achieve complete recovery, we provide the following update on the current situation.

1. Incident Overview

In the early hours of Tuesday, May 20, we detected unauthorized modifications to files on some servers and PCs within our company and group companies. Subsequent investigation confirmed a cyberattack involving ransomware, and in order to respond swiftly, we established an emergency response headquarters. As part of our countermeasures to prevent the spread of damage, we implemented network isolation measures, which resulted in partial system unavailability within our company and group, leading to disruptions in business operations. We have since commenced a detailed investigation with the assistance of external specialists.
We have also reported the incident to law enforcement and are coordinating with relevant government agencies, while continuing efforts to minimize the impact on stakeholders.

2. Current Status and Future Actions

Starting Friday, May 23, we have begun gradually resuming operations for certain businesses where safety has been confirmed. As of Tuesday, June 3, we are continuing restoration efforts for the remaining PCs, systems, networks, and other infrastructure to normalize operations.
According to the investigation conducted by external specialists, there has been no confirmation of information leaks involving our group or our business partners. Production and shipment of products have also been gradually resuming.

We have confirmed that the incident was caused by an external attacker infiltrating our group’s network and activating ransomware. To prevent recurrence, we will implement comprehensive countermeasures, including virus scans on all servers and PCs, password resets, deployment of early detection tools, reinforcement of our incident monitoring framework, and enhancement of employee training programs.
We are continuing to assess the potential impact of this incident on our business performance. Should it be determined that there will be a significant effect, we will make a prompt disclosure. We will continue to provide updates as new information becomes available.

Once again, we sincerely apologize for the inconvenience and disruption caused to our business partners and all those concerned.

For further information, contact:
Media Relations Group, Brand Communication Department (Phone: 81-3-6263-8002)