JTEKT

COMMUNICATION TO CUSTOMERS AND SUPPLIERS - update

Follow-up Report on the Ransomware Incident and Data Breach at our European operation – 19 August 2025

Dear Valued Customer/Partner,

We hope this message finds you well.

We would like to express our sincere appreciation for your continued support.

As previously reported, our European operation (hereinafter referred to as the "European operation") experienced a cyberattack involving ransomware. We have now confirmed that information believed to have been stored on our servers has been published on a specific website.

The details confirmed at this time are outlined below.

We deeply apologize for the concern and inconvenience caused to our business partners and all related parties.

Although we have not engaged in negotiations with the attackers since the incident was discovered, we sincerely apologize once again for the current situation.

Additionally, we plan to publish an official statement regarding this matter on our corporate website in the coming days.

Yours Sincerely,

Details:

1. **Incident Discovery Timeline**
   On July 21, 2025 (Japan time), an alert from the security system at our European operation prompted an investigation, which confirmed that several servers had been compromised with ransomware
   Together with external specialists, we have been investigating whether any data was stolen. On August 10, 2025 (Japan time), we confirmed that data believed to have been stolen was published on a specific website.

2. **Scope of the Attack**
   - Multiple servers at the European operations: Encrypted by ransomware, with potential data leakage
   - Multiple PCs: Encrypted by ransomware, with potential data leakage

The security system detected the attack and immediately disconnected the affected devices from the network.
At the same time, network connections between the European Office and other regions, including our Japan headquarters, were severed, preventing the spread of the attack to other regions.

3. **Preventive Measures**
   To prevent further damage, the affected business systems and PCs were isolated from the internal network at the time of the incident.
   We are gradually reconnecting servers and PCs that have been confirmed safe by external specialists.

4. **Identification of Confidential Data**
   We are currently working with external experts to identify the data that was leaked and published.

5. **Cause of the Incident**
   We are conducting a detailed investigation in collaboration with external specialists. A separate report will be provided once the investigation is complete.

6. **Impact on Deliveries**
   Production is currently proceeding without issues, and there has been no impact on deliveries to our customers.

7. **Inquiries regarding this matter**
   Please contact your respective sales representative