Regarding the Possibility of Information Leakage at Overseas Group Companies

2025-11-10

SATO CORPORATION

We regret to inform you that a cybersecurity incident has occurred within our managed cloud service environment, and there is a possibility that information related to business partners, including personal data, may have been compromised. Following confirmation and investigation after the facts came to light, we are making this announcement today.

Personal information such as names, email addresses, postal addresses, and telephone numbers of employees of our overseas group companies (as described below) and business partners, as well as information related to business transactions, may have been exposed. At this time, there is no confirmation that any “special category” personal data under GDPR has been compromised.

1. Incident Overview

At 09:35 AM (UTC) on Sunday, October 12, 2025, we received a report from the service provider managing our cloud service environment that a cyberattack had exploited a zero-day vulnerability (CVE-2025-61882) in Oracle E-Business Suite. Preparation for the attack was detected in early July 2025, and the initial intrusion occurred in August 2025. During this time, unauthorized access was gained, and confidential information may have been exfiltrated.

The identified vulnerability has since been remediated, and we have been assured by the service provider that our managed environment is no longer under attack. Systems of our overseas group companies and systems in Japan continue to operate normally, and no impact on business operations has been identified

2. Measures Taken

The exploited zero-day vulnerability (CVE-2025-61882) was patched immediately after an emergency fix was released and applied on October 5 and 6. Following the initial response, the service provider confirmed that no further attacks had been carried out on our environment and that it was secure. Subsequently, we strengthened our monitoring system while simultaneously considering additional security measures to prevent recurrence.

We have reported this matter to the relevant local data protection authorities and are fully cooperating in addressing the incident.

3. Information Regarding Affected Data

The systems of our overseas group companies process and store personal data necessary for business operations, such as names, email addresses, postal addresses, and telephone numbers.

The affected system contains information required for normal business activities, including order placement, shipping, delivery, and accounts receivable/payable. It does not include passwords or details such as product firmware information.

Our company and its overseas group companies handle personal information in accordance with applicable laws and are committed to its protection.

This notice serves as an initial report. Any additional information identified through further investigation will be disclosed promptly as soon as it becomes available.

We take this matter seriously and will make every effort to prevent recurrence by working closely with the service provider and implementing all necessary measures.

4. Data of the following group companies may have been affected

The overseas group companies that were using the affected business systems are listed below.

USA	SATO America, LLC
Singapore	SATO Asia Pacific Pte. Ltd.
	SATO Global Business Services Pte. Ltd.
Malaysia	SATO Auto-ID Malaysia Sdn. Bhd.
Europe	SATO Europe GmbH (Germany, Italy, Netherlands, Spain)
	SATO Central Europe (Poland)
UK	SATO UK Ltd.

5. Notice to Potentially Affected Individuals

We are individually contacting all parties who may have been affected. In addition, we have established a dedicated point of contact for inquiries regarding this matter. For those we are unable to reach individually, this announcement shall serve as official notification.

We ask all individuals who may be affected to remain vigilant against fraudulent activities such as phishing scams and identity theft.

We sincerely apologize for any inconvenience and concern this incident may have caused. Moving forward, we will continue to strengthen our security measures and work diligently to prevent recurrence.

6. Contact Information

If you have any questions or require additional information, please contact us at:

csirt-inquiry@sato-global.com