KEPCO Confirms Breach Affecting About 1.5 Million People



South Korea's state-owned utility KEPCO says an external attacker stole data from its customer portal and supplier platform, including payment details. The case is a useful prompt to review portal and third-party data exposure.

- KEPCO disclosed a breach affecting roughly 1.5 million people, involving its KEPCO ON customer portal and its SRM supplier platform.
- From KEPCO ON, data of 650,487 people was taken, including IDs, contact details, card and bank account details and billing information.
- From the SRM platform, data of 869,761 individuals was taken, including names, ID numbers, email addresses and company contact details.
- KEPCO did not say how the attacker gained access or confirm that AI was used; South Korea's PIPC

has opened an investigation.

- The company suspended the affected services, blocked external access and notified the affected individuals and authorities.

Korea Electric Power Corporation (KEPCO), a South Korean state-owned utility, has disclosed a data breach affecting approximately 1.5 million people. The company attributes the incident to an external attacker.

What was affected

Two systems were involved: KEPCO ON, the integrated customer service portal, and the supplier relationship management (SRM) platform used for procurement and service contracts. From KEPCO ON, data of 650,487 people was stolen, including names, addresses, phone numbers, unique ID numbers, customer numbers, card details, bank account details and billing and payment information. From the SRM platform, data of 869,761 individuals was taken, covering names, ID numbers, email addresses, company addresses, employee IDs and phone numbers, including KEPCO staff and employees of partner companies.

Response and open questions

KEPCO says it suspended the affected services on discovery, blocked external access, reviewed the systems and carried out remediation. On November 20 it confirmed that data had been exfiltrated. It has notified affected individuals and reported to the relevant authorities, and will share details on financial information exposure with government and financial institutions.

The disclosure followed a dark web post on November 19 by a user using the handle Noiem, who reportedly claimed to hold KEPCO user, supplier, bidding and contract data. South Korea's Personal Information Protection Commission (PIPC) has opened an investigation and has not attributed the breach to that user. KEPCO has not said how access was gained, nor confirmed that AI was used, although it cited the growing sophistication of AI-driven attacks.

Why it matters

The case shows how customer portals and supplier platforms can hold payment, identity and contract data in one place. Organisations in the Kingdom with similar portals can use it as a prompt to check their own exposure.

What to do now

1. Inventory customer portals and supplier platforms and map which personal, payment and contract data each one stores.
2. Review whether card and bank account data is retained, and minimise, tokenise or mask it where possible.

3. Check access controls, logging and monitoring on these platforms, including external access paths and exfiltration alerts.
4. Confirm that your incident plan covers service suspension, notification of affected individuals and reporting to SDAIA and the relevant sector regulator under PDPL.
5. Monitor dark web sources for claims involving your organisation and agree a process for verifying sample data.