Kawasaki
Powering your potential

News Release

Kawasaki Heavy Industries, Ltd.

December 28, 2020

Concerning Unauthorized Access to Kawasaki Group

Tokyo, December 28, 2020 — Kawasaki Heavy Industries, Ltd. announced that it was subject to unauthorized access from outside the company. As a result of a thorough investigation, the company have discovered that some information from overseas offices may have been leaked to external parties.
At this time, the company has found no evidence of leaking information to the external network. However, due to the fact that the scope of unauthorized access spanned multiple domestic and overseas offices, it took a considerable amount of time until the company can formally announce the incident. We sincerely apologize for this delay and for the inconvenience and concern to customers and other related parties.

1. Summary

On June 11, 2020, an internal system audit revealed a connection to a server in Japan from an overseas office (Thailand) that should not have occurred. Within the same day, communication between the overseas office and our Japan office was fully terminated considering as a case of unauthorized access. However, other unauthorized accesses to servers in Japan from other overseas sites (Indonesia, the Philippines, and the United States) were subsequently discovered. We have therefore enhanced monitoring operations to accesses from overseas offices and tightened access restrictions to block unauthorized accesses. Since then, we have continued to strengthen company-wide security measures.

2. Course of events

June 11	Identified unauthorized access from an overseas office in Thailand by an internal system audit of Japan office Terminated internal network between an overseas office in Thailand and Japan office Initiated investigation to determine the scope and target of the intrusion
June 15	Confirmed a possibility of data breach to external parties through the overseas office in Thailand
June 16	Confirmed unauthorized access from the overseas office in Thailand to multiple servers in the Japan data center
June 24	Confirmed unauthorized accesses from other overseas offices in Indonesia and Philippines to the Japan office Connection between both overseas offices and Japan office cut off

July 8	Confirmed suspicious unauthorized accesses from overseas office in the United States to the Japan office Added additional restriction to network between the overseas office in United States and the Japan office
August 3 onward	Implement enhanced network communication restrictions at all overseas and Japan office Conducted a thorough security soundness inspection of approximately 26,000 terminals in Japan and Thailand network (Normalization confirmed by the end of October)
October 5 onward	Conducted a thorough security soundness inspection of approximately 3,000 terminals in overseas offices network (excluding Thailand) where breaches possibly occurred (security threat eradiation confirmed by the end of November)
October 30	Confirmed by continuous network monitoring that no further unauthorized accesses to the Japan office occurred after August
November 30	Restored network communication terminated between overseas offices and the Japan office
December 21	Continued monitoring of network traffic after resuming the connection of the restricted overseas offices and confirmed that there were no suspicious transactions and activities from the overseas offices mentioned above.

3. Impact

Because Kawasaki handles important sensitive information such as personal information and social infrastructure-related information, information security measures have been a top priority for the company. However, the unauthorized access in question had been carried out with advanced technology that did not leave a trace.

To this end, since the confirmation of unauthorized access, Kawasaki special project team engaged with an independent external security specialist firm has been investigating and implementing countermeasures. Their investigation confirmed a possibility that information of unknown content may have been leaked to a third party. However, at the present time, we have found no evidence of leaking information including personal information to external parties.

Customers who may have been affected by this unauthorized access are being contacted individually.

4. Future actions

In addition to continuing to tighten monitoring and access control in communication networks between our overseas offices and domestic offices, the Cyber Security Group (established on November 1, 2020), which is under the direct control of the corporate president, will strengthen security measures, analyzing the latest unauthorized access methods, to prevent recurrence.

- End of document –