Nidec Corporation

June 27, 2024

# Security Incident at a Nidec Group Company (the Second Report)

Nidec Corporation (the "Company" or "we") today released its second report regarding the damage caused by the ransomware attack at Nidec Instruments Corporation ("Nidec Instruments"), a Nidec Group company – the incident announced on June 10. We deeply apologize for all the inconveniences and concerns that this incident has caused to our business partners and others concerned.

The Company has confirmed that this incident has caused no impact to us or any Nidec Group companies other than Nidec Instruments Corporation. We are committed to taking action for a prompt recovery from this incident, while improving the entire Nidec Group's information security system, and launching every available measure to prevent similar cases in the future.

Please see the next pages for the press release issued by Nidec Instruments.

**Nidec Instruments Corporation**

June 27, 2024

# Nidec Instruments Warns of Possible Personal Information Leak Due to Recent Unauthorized Access to the Company's Information System, Makes an Apology for the Incident

Thank you very much for your continued support for Nidec Instruments Corporation ("Nidec Instruments" or "we").

As announced on June 10, 2024 on our and Nidec Corporation's websites under the titles, "Security Incident at a Nidec Group Company" and "Security Incident at Nidec Instruments Corporation" respectively, Nidec Instruments and companies in our group (the "Nidec Instruments Group") were hit by a cyberattack by an external malicious attacker (the "attacker"), falling victim to ransomware, which encrypted files in our multiple servers.

This latest press release is to report to you on, among other information, facts that have been revealed since our previous announcement, and the information that the Nidec Instruments Group has obtained so far. As explained in Section 5 below, we will make sure to inform you of any new fact going forward. As explained above, this incident has made no impact to Nidec Corporation or any of its group companies other than Nidec Instruments. Once again, we deeply apologize for all the inconveniences and concerns that this incident has caused to our business partners and others concerned.

1. Details of the unauthorized access
   On May 26, 2024, a ransomware-caused unauthorized access was made to our business operation system and others under our ownership, encrypting information in our system. After the June 10 announcement, we continued our investigations into our servers, etc., to reveal that: part of the data in the servers, file servers, etc. of the internal systems of Nidec Instruments and other Nidec Instruments Group companies in Japan, *i.e.*, Nidec Material Corporation, Nidec Instruments Service Engineering Corporation, Tokyo Maruzen Industry Co., Ltd., Nidec Instruments Akita Corporation, Sunseiki Co., Ltd., and Nidec Music Box Museum Suwanone, and of Nidec Instruments' overseas subsidiaries* was encrypted; and the attacker accessed information under the Nidec Instrument Group's ownership, and thus it is undeniable for part of the information may have leaked to outside parties.

   *The following nine companies were not affected by the ransomware attack, as their network configurations are different from that of the Nidec Instruments Group's.

   (i) SCD Co., Ltd.
   (ii) SCD (Guangzhou) Co., Ltd.
   (iii) SCD (Hong Kong) Co., Ltd.
   (iv) Nidec Instruments (America) Corporation
   (v) Nidec Instruments México S.A. de C.V.
   (vi) Nidec Instruments (Europe) GmbH
   (vii) Nidec Genmark Automation, Inc.
   (viii) Nidec Genmark Automation (Suzhou), Inc.
   (ix) Nidec Genmark Automation (Europe), Inc.

2. Information subject to possible leak, etc.
   At present, investigations are underway regarding the specific contents of information that may have leaked, etc. as a result of this incident.

3. Events that unfolded regarding this incident
   The actions that the Nidec Instruments Group has launched in response to the incident are as follows:

   - On May 26, an employee of Nidec Instruments' information systems department detected an attack caused by this incident. On the same day, as part of its initial measures against the attack, the department utilized EDR software and anti-malware software to remove the malware program that caused the incident, while Nidec Instruments formed an internal response team for this cyberattack.

- On May 27, based on its instruction to all Nidec Instruments Group employees, Nidec Instruments confirmed that the malware program that caused this incident had not been activated in any of the Nidec Instruments Group's PCs. On the same day, we recovered our data from their backup data to build a minimal system to continue our business operations with outside parties.

- On May 28, based on that fact that it is undeniable that part of the Nidec Instruments Group's information may have leaked to outside parties, we started reporting to, and consultations with, the Nagano Prefectural Police on this matter. Additionally, from this day on, we recovered our internal core and peripheral systems, and launched, among other actions, measures to recover data in collaboration with security product vendors.

- On June 03, after requesting an outside security-specialized agency, we started investigations exclusively into facts related to this incident. While launching an attack on Nidec instruments, the attacker who caused the incident demanded to Nidec Corporation, our parent company that it pay ransom. However, we have not made any such payment so far, as, among other reasons, we must never make any payment to antisocial forces.

- On June 10, we issued a press release titled "Security Incident at a Nidec Group Company" and "Security Incident at Nidec Instruments Corporation" on our and Nidec Corporation's websites. On the same day, we submitted a preliminary report to our personal information protection committee, while making an official internal notice with the same contents as those of the report to our employees. On the following day of June 11, other Nidec Instruments Group companies submitted their preliminary reports to the personal information protection committee.

- On June 12, we started consultations with external attorneys, while receiving an initial investigation report from the outside security-specialized agency.

- Since then, we continue to work with the external security-specialized agency and the outside attorneys to proceed with our recovery measures and other actions.

- On June 18, we confirmed a download link apparently related to the Nidec Instruments Group on the attacker's information-leak website, and that information on our group was downloadable. Investigations thereafter confirmed that the information is not downloadable as of now. We continue to work with the outside security-specialized agency to monitor the information-leak website constantly. We will contact and talk with individual customers that have been affected by this incident as soon as details are identified.

4. Results of the investigations
   (1) Extent of the damage caused by the incident
   As explained in Section 1, "Details of the unauthorized access," above, we have confirmed that part of not only Nidec Instruments' but also the Nidec Instrument Group's data have been encrypted in this incident. So far, there has been no report on secondary damage, such as unauthorized use of information, attributable to this incident.

   (2) Cause of this incident
   We believe that this incident was caused after the ID and password of the system's administrator were somehow acquired by the attacker, who then accessed our company's business system.

5. Current situation and going forward
   As an emergency measure to prevent further damage by this incident, we have separated the PCs, servers, etc. that were subjected to the cyberattack from the rest of the Nidec Instruments Group's network, and enhanced the passwords of the accounts of all the users of devices concerned.

   We will continue to consult with the external security-specialized agency and outside attorneys to proceed with our investigations and other activities, and reveal relevant facts. Thereafter, based on the results of future investigations and the progress of our actions going forward, and based on advice from the external security-specialized agency and the outside attorneys, we will launch measures to first build, in early July or so, an environment where our customers and business partners can work with us safely and securely.

   In the meantime, we will continue to report to, and collaborate with, the personal information protection committee, the police, and other organizations, and, based on the results of the investigation, issue another report after identifying relevant facts.

6. Other information
   As the attacker of this incident is expected to take action such as distributing information, please make sure not to open any suspicious email, or access any URL, etc. therein.

7. For inquiries on the above matter, please contact us at Nidec Instruments' pilot number at *81-266-27-3111. Thank you.