October 17, 2024
Nidec Corporation

Security Incident at a Nidec Group Company (Report No. 2)

Nidec Corporation today announced that Nidec Precision Corporation has released the latest information regarding the damage caused by data leakage that occurred due to an unauthorized access to Nidec Precision Corporation's Vietnamese subsidiary on August 12. We deeply apologize for the inconvenience and worry that this incident must have caused to those concerned.

Please see below for the latest press release by Nidec Precision Corporation.

October 17, 2024
Nidec Precision Corporation

Security Incident at Nidec Precision Corporation (Report No. 2)

Thank you for your continued support for Nidec Precision Corporation ("Nidec Precision").

As announced in our August 12, 2024 press release (Please click here for the announcement, or the "first report") on our company's website, Nidec Precision Vietnam Corporation ("NPCV"), our business base in Vietnam, suffered an unauthorized access from a vicious external criminal ring (the "external criminal group"), which stole documents and files in NPCV's server, and which demanded ransom in exchange for them. In this blackmailing case, after Nidec Precision refused to accept the external criminal group's demand, the external criminal group went on to disclose those stolen documents and files on a so-called dark website, enabling third parties to access them (the "Incident").

This latest report features the results of our investigations into the Incident so far. We deeply apologize that it has taken time until now, as we wanted to provide concerned parties with accurate information, and that this Incident must have caused inconvenience and concern among many.

1. Overview of the incident
On August 05, 2024, an external criminal group informed us that they had made an unauthorized access into NPCV's network, and stolen documents and files stored in its server. This message was followed by the group's demand for "ransom." Investigations by outside experts and Nidec Precision discovered that part of NPCV's information had been disclosed on a so-called dark website, with access by third parties possible. However, there has been no damage (new cyberattacks, files being encrypted, etc.) since those documents and files were disclosed on the website.

In addition, no damage related to the Incident has been confirmed at Nidec Precision's group companies other than NPCV, or at Nidec Corporation or its group companies. For more details on the countermeasures against the Incident so far, please see Section 7, "History of the countermeasures against the Incident so far."

2. The information disclosed by the external criminal group
Among the files about which Nidec Precision cannot deny the possibility for the external criminal group to have viewed, the information that we identified, by conducting investigations via every possible measures, as having disclosed by the external criminal group is as follows:

Number of the files: 50,694
Types of the stolen information: NPCV's internal documents, letters from our business partners, documents related to green procurement, labor safety and hygiene policies (work, supply chain, etc.), business transaction-related documents (order forms, invoices, receipts, etc.), and contracts among others
Nidec Precision will contact relevant individual business partners on the leaked information.

3. Causes and countermeasures
(1) Causes
We believe that the external criminal group must somehow illegally acquired the IDs and passwords of users of NPCV's general domain accounts, and stolen files that can be viewed with those accounts' authority.

(2) Countermeasures
As temporary countermeasures, we scanned all electronic terminals, reset passwords, and reviewed the access authority to the server, at all of Nidec Precision's group companies, while, at NPCV, suspending the use of the VPN* device suspected of having allowed the cyberattack first, until sufficient countermeasures are in place.
*VPN (virtual private network): A dedicated online network that only specific people can use.

4. Presence/absence of actual/possible secondary damage, and its details
Among the information that was or may have been leaked, etc., there is no information that may directly cause secondary economic damage. In addition, at this moment, we have not confirmed direct secondary damage, such as improper use of information, attributable to the Incident.

If you receive any suspicious email, etc. sent by, for example, someone falsely representing Nidec Precision's business group or claiming the Incident's attacker, please make sure not to open the message, or access the URL, etc. in it.

5. Preventive measures
Going forward, we will consult with external professional security organizations and attorneys as we launch such actions as enhancing our security system, reeducating our employees, and launching preventive measures, to build a business environment about which our business partners can feel safe and secure.

6. Contact information
For inquiries on the Incident, please contact:
General Affairs & HR Department, Head Office, Nidec Precision Corporation
Tel.: +81-3-3965-1115
Business hours: 09:00 – 17:00 (on weekdays only)

7. History of the countermeasures against the Incident so far
The history of our business group's countermeasures against the Incident are as follows:
- August 05: Nidec Precision receives a message from the external criminal group claiming responsibility for the Incident.
- August 06 – 08: Nidec Precision starts consultations with an outside security incident expert, and launches investigations into the incident.
- August 09: The investigation reveals that information likely to have been stolen from NPCV is on the website (the "leak site") claimed by the external criminal group to be where they had posted a sample of the stolen information, and that the information can be downloaded by a third party.
- August 12: Based on the status at the point in time, Nidec Precision issues its first report on the Incident on the company's website.
- August 15: NPCV files a report to the local police department of Vietnam on the damage caused by the information leak.
- August 28: Nidec Precision starts consultations with an outside attorney. Communications thereafter confirms that there is no obligation for the company to file a report based on Japan's Act on the Protection of Personal Information.

- September 06: Amid ongoing investigations by an outside investigation firm, and after consultations with an outside attorney, NPCV files a report to the Cybersecurity and Hi-tech Crime Prevention Division of Vietnam's Ministry of Public Security, based on the Decree on Personal Data Protection.
- September 07: Nidec Precision confirms that the external criminal group has posted additional information on the leak site, and posted a message about it in the social media.
- September 09: Nidec Precision confirms that the information stolen by the external criminal group is downloadable on the leak site.
- September 12: NPCV files a damage report on additional information leak to Vietnam's Cybersecurity and Hi-tech Crime Prevention Division.

Once again, we deeply apologize for all the trouble and inconvenience that this incident must have caused to our customers and other people concerned.