November 28, 2023
Mazda Motor Corporation

Possible Leak of Personal Information Due to Unauthorized Access (Follow-up Report)

On September 15, 2023, Mazda Motor Corporation reported the possibility of a leak of personal information due to unauthorized access to one of the Company's servers and issued an apology and notification to stakeholders (see News Release: Apology and Notification Regarding Possible Leakage of Personal Information Due to Unauthorized Access). In the same press release, we announced that a third-party security firm would conduct an investigation of the incident. The security firm has completed its investigation and we would now like to report details of the investigation and remedial measures we intend to take.

As we indicated in our initial report of the incident, no customer information is stored on the server concerned and, therefore, there is no possibility that customer information was leaked. The server that was the subject of the unauthorized access stores information about Mazda employees, employees of group companies and cooperating companies and account information of persons in charge at Mazda suppliers, and it was determined that some of this information may have been leaked externally.

Furthermore, while the matter has yet to be confirmed, there is a possibility that personal information stored on the server concerned may be misused for purposes such as forwarding phishing and spam email. Persons who receive suspicious emails are requested to take cautionary measures.

We again sincerely apologize to all our stakeholders for the significant inconvenience and worry this incident has caused.

Results of the Investigation and Remediation

Following the incident, an external security firm conducted an investigation of the Company's servers and network system. The investigation confirmed that vulnerabilities in a server installed in the company network were exploited and became the route of unauthorized access to the Company. The investigation further confirmed that a third party engaged in unauthorized operations on the directory server, which manages account information such as user IDs and passwords of employees of Mazda, group companies and cooperating companies.

Operation of the server that had been the route of unauthorized access to the directory server was suspended after confirmation of the incident.

Furthermore, investigation of the company servers confirmed that there was no other unauthorized access to servers other than the directory server and the server that was the route of unauthorized access. However, because the investigation confirmed a history of unauthorized access to the directory server, all user ID passwords were changed to prevent further damages. Additional precautionary measures including enhanced monitoring of the directory server were also put in place to prevent further damages. Since the implementation of these measures, no unauthorized access has been detected.

Remedial Measures

We at Mazda recognize this incident as a serious management issue and we are determined to make every effort to prevent a recurrence.

As a specific measure to prevent unauthorized access that takes advantage of vulnerabilities, we will improve our procedures for dealing with such incidents by introducing Attack Surface Management (ASM)[1] to enhance our detection capability in the event of external unauthorized access. Furthermore, we will strengthen procedures for managing OS and software version information to keep them up to date to eliminate vulnerabilities.

In addition, we will accelerate the implementation of multifactor authentication (MFA)[2] and we will introduce a system for detecting and rapidly responding to unauthorized access to the internal network and misconduct misusing user IDs.

By continually implementing these measures, we will make improvements to the Company's system services, which all stakeholders will be able to use with a sense of security.

We again sincerely apologize to all our stakeholders for the significant inconvenience and worry this incident has caused.

<Inquiries regarding this matter>

Please use the inquiry form below for any inquiries concerning this matter.

Inquiry form: https://mag.mazda.jp/enq/pub/common/svaccinqen

(ASM)[1]: A series of processes for discovering IT assets that can be accessed from outside an organization (via the internet) and continually detecting and assessing vulnerabilities and other risks that exist in these.

Source: Cybersecurity Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry

"A Guide to Introducing Attack Surface Management (ASM)"

(MFA)[2]: A method for verifying the identity of an individual by using multiple types of information such as password, telephone number or other information during log on to a service or application.

# # #