July 6, 2026

＜Press Release＞

KDDI Corporation

Notice Regarding Unauthorized Access to Email System for ISP Providers

We would like to express our sincere apologies for the significant inconvenience and concern caused to Internet Service Providers (hereinafter, "ISP providers") and their customers and many other stakeholders regarding the unauthorized access (hereinafter, "this unauthorized access") (Note 1) to the email system (hereinafter, "the system") that we provide to ISP providers, which we announced on June 23, 2026.

We confirmed this unauthorized access on June 17, 2026. On the same day, we modified the system to prevent further damage. We have identified the suspected points of this unauthorized access and implemented technical defensive measures.

Additionally, on June 24, 2026, we were requested by the Ministry of Internal Affairs and Communications to submit a report based on Article 166, Paragraph 1 of the Telecommunications Business Act (Note 2), and we submitted the report today, July 6.

In conjunction with this, we are proceeding with an analysis of the scope of impact and the causes, customer support in cooperation with ISP providers, and measures to prevent recurrence, as detailed below.

Our mobile and fixed internet email services (au mail, UQ mobile mail, au one net mail) are built on different infrastructure and are not affected by this unauthorized access, nor has any information been leaked from them.

1. Timeline and Cause of This Unauthorized Access

This system is an email platform developed by our company for ISP providers, offering a comprehensive suite of features including email account management, email sending/receiving, webmail functionality, and email data storage.

This unauthorized access was caused by the exploitation of a vulnerability (hereinafter, "the vulnerability") in third-party software (hereinafter, "the software") that we had

incorporated as part of this system. It began on May 16, 2026, for some ISP providers. We confirmed this unauthorized access on June 17, 2026. On the same day, we modified the system to prevent further damage and addressed the vulnerability.

Our investigation revealed that this vulnerability was not recognized by the software vendor as of June 17, 2026, when we identified it. The software vendor has reported this vulnerability to public institutions and is working towards disclosing the information.

2. Confirmed Leaked Information and Number of Affected Individuals

Of the email-related information whose potential leakage was announced on June 23, 2026, the information and number of individuals confirmed to have been leaked are as follows:

1) Leakage of email addresses created in this system

Number of affected individuals: 12,231,954

2) Leakage of system passwords

Number of affected individuals: 7,616,173

※ The number above is a subset of the number in 1).

3. Current Response Status

Following confirmation of the unauthorized access, we have been working closely with ISP providers to promptly facilitate password changes for affected customers' email accounts, thereby enhancing the protection of customer information and helping to prevent any potential future risks.

To date, a large number of password changes have already been completed, primarily by customers who regularly use email services. In addition, to ensure the security of all customers, including those who do not use email services frequently, ISP providers are moving forward with mandatory password changes, aiming for completion within the next day or two.

In addition, we are also supporting each ISP provider with their customer support efforts.

4. Measures to Prevent Recurrence

(1) Implemented Measures

To prevent further damage from this unauthorized access, we modified the system on June 17, 2026. Furthermore, on June 21, 2026, we completed the implementation of EDR (Endpoint Detection and Response) on all servers controlling external communications to enhance detection of unauthorized access. In addition, on June 23, 2026, a forensic

investigation by a third-party organization confirmed that there were no suspicious traces other than this vulnerability. Through these measures, we promptly took steps to ensure security.

（2）Future Measures

As continuous future measures, we will analyze the design documents and programs of this software, utilizing AI and other tools, to comprehensively check for potential issues. Based on the results of this analysis, we will thoroughly confirm that there are no defects or flaws in the software.

In addition, as a fundamental initiative, while considering the impact on customers using conventional email software, we will work with ISP providers to rapidly transition to communication standards with higher security strength, thereby contributing to the overall improvement of security across the industry.

（Note 1）Press Release on June 23, 2026

Unauthorized Access to Email System for ISP Providers

https://newsroom.kddi.com/english/news/assets/2026/kddi_nr-1114_4644/kddi_nr-1114_4644_pdf_01.pdf

（Note 2）Ministry of Internal Affairs and Communications, June 24, 2026: "Request for Report from KDDI Corporation" (In Japanese only)

https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000281.html

End