Documented incident timeline

API authorisation weakness in WAYSCloud Cloud Management API

INCIDENT REFERENCE	REGULATORY SUBMISSIONS
WAYSCLOUD-TR-2026-0034	**Initial: 58dd4a567918 | Supplementary: 2a3ec7cb24b0**

Sequence of verified actions

28 Oct 2025	Historical source review Original authorisation pattern traced to the initial code. First public exploitability cannot be independently dated.
22 Nov, 18:08	Discovery First documented internal identification; scope and risk assessment begin.
22 Nov, 18:40–18:56	Initial correction First corrective code changes recorded; no production fix deployed at this point.
22–23 Nov, overnight	Investigation and testing Code review, permission analysis, negative security tests and release preparation continue.
23 Nov, 05:41	Initial authority notification First notification to Datatilsynet. Ref. 58dd4a567918.
23 Nov, 06:32–08:56	Release verification Rotation and authorisation changes integrated; combined tests and review completed.
23 Nov, 09:06	Production remediation Corrected release deployed, service health checked and missing action permission rejected (HTTP 403).
23 Nov, daytime	Impact assessment Historical usage, IPs and resources correlated; external scope narrowed to two accounts / four credentials.
23 Nov, 18:26	Customer notification First external customer individually notified through electronically signed communication.
23 Nov, 18:27	Customer notification Second external customer individually notified through electronically signed communication.
23 Nov, 18:39	Supplementary authority notification Additional submission to Datatilsynet including updated findings and redacted supporting documents. Ref. 2a3ec7cb24b0.

Assessment: A genuine authorisation weakness was corrected and verified in production. No unauthorised exploitation or compromise of personal data was identified in the available evidence; historical per-credential attribution is incomplete.