



Bremanger Dam



Discovered: 7 April 2025

Sector: Aquaculture:
hatchery water supply

Systems Reached:
External login to valve control

Scale: One dam at Risevatnet,
Bremanger; one valve

Initial Access Vector: Probably a
weak password, in the owner's words

Attacker: A pro-Russian hacktivist
group (PST); not publicly named

Root Cause: Undisclosed

Malware: None reported

Operational Impact:
Valve fully open; access lasted just
under four hours (NTB). How it was
closed is undisclosed.

Financial Impact: Undisclosed

Process Impact: 497 litres a second
above minimum flow into Riselva, per
the owner; flood calculation about
20,000. No damage to fish or plant
(owner); no injuries (Reuters).

Cross Reference: Tczew · Oldsmar ·
US Water Campaign

In April 2025 someone reached the remote login of a small dam in western Norway and opened its valve all the way. The dam supplies a fish hatchery, not a power plant. Nothing flooded, and the owner said plainly how it happened.

Bremanger is the rare small incident with more than one witness. A hacktivist video is a claim; here it met an owner who described the event to the press, police who examined the video, and a security service that wrote the case into its threat assessment. The effect deserves its true size: one minimum flow valve on a hatchery's dam stood fully open for just under four hours, by the owner's account, and nothing flooded.

The valve had an external login, and the owner's view is that a weak password was probably enough. The question is not how strong the password was but why a valve that needed only a schedule and a guard would answer anyone on the internet. That reading is BlastWave's analysis. The retelling did worse: the valve became a floodgate, the hatchery became energy infrastructure, and pro-Russian actors became Russia. Our own first volume did all three.

What is not known: No Norwegian authority has published how the login was reached. The owner said a weak password was probably to blame; the police said nothing on method and closed the case in October 2025 without identifying anyone. Neither PST nor Kripos has publicly named the group whose watermark is on the video, and no government document attributes the operation to the Russian state. The duration and flow are the owner's figures, not a published log. How the opening was spotted, how and by whom the valve was closed, and what it cost are undisclosed.

Recommendation

1. Take the path away

A valve that runs on a schedule, with a guard within driving distance, does not need a login that answers the internet. Put it where strangers cannot find it.

2. Remove credential-only access

Any remote change to discharge needs a named person, a second factor and a logged, time-boxed session. A local limit on remote opening is BlastWave's suggestion.

3. Let the watchers read one way

Level, flow and alarms leave the dam over a one-way path, so checking on it from town never needs a door that can also open it.



The Orchard Timer
Embedded audio/file-013.m4a



Bremanger Dam Short
External Link – Opens in Browser

Sources: PST, National Threat Assessment 2026, p. 27 · NTB, 10 Jun 2025 (owner's account) · Energiteknikk, 11 Jun and 14 Aug 2025 · Reuters, 13 Aug 2025 (via ABC News) · iLaks, 3 Oct 2025 (case closed, per NRK).

Soft Spots: Duration and flow are the owner's figures via the press; the weak password is the owner's "probably." No source says who closed the valve. That the login answered the internet is BlastWave's inference.