

(English version)

**Question for written answer E-001748/26
to the Commission
Alvise Pérez (NI)
(29 April 2026)**

Subject: New security breach at the Commission and potential mass exposure of personal data

On 27 March 2026, the Commission confirmed that there had been a cyberattack against the cloud infrastructure hosting part of its web presence on Europa.eu and admitted that early findings suggested that data had been taken from those websites.

CERT-EU subsequently confirmed that the published dataset contained names, last names, usernames and email addresses, predominantly from the Commission's websites but potentially also pertaining to users from multiple EU entities.

In view of the above:

1. Can the Commission say how many individuals and how many EU entities have already had their data compromised by another major security breach of systems it is responsible for?
2. Why did the Commission not identify and block in time a breach that, according to CERT-EU, enabled a significant volume of data to be exfiltrated?
3. Which political and technical decision-makers will bear consequences for this fresh demonstration of vulnerability in the Commission's own systems?

Submitted: 29.4.2026

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(23 June 2026)**

The cyberattack targeted the Commission's Drupal cloud hosting service, affecting 39 internal clients and 18 other EU entities ⁽¹⁾. Given that the processing activities were carried out under the responsibility of multiple independent operational controllers, risk assessments and subsequent actions for the personal data they control were carried out by those entities themselves. The Commission is working closely with affected parties to ensure appropriate measures are taken to mitigate the impact.

The breach occurred outside of any Commission-monitored systems, with attackers exploiting compromised credentials from Aqua Security to deploy a malicious version of the Trivy security scanner. This allowed them to steal credentials, conduct reconnaissance, and expand their activities.

The attack's sophistication enabled threat actors to evade detection temporarily despite the Commission's robust security measures. The Commission is continuously improving its security protocols, including account management, behavioural monitoring, and decoy techniques, while investigating the incident to identify and address vulnerabilities.

The Commission takes cybersecurity incidents extremely seriously and is collaborating with the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU) and other bodies to strengthen cybersecurity. Lessons from this incident will inform future improvements to better protect systems and data.

⁽¹⁾ All information included in this reply is based on the current status of the investigation, which the Commission is finalising.