EUROPE

Hackers breached the European Commission by poisoning the security tool it used to protect itself

April 4, 2026 - 1:45 pm

STORY BY
Allison Steffens Herrera

CERT-EU has attributed a major data breach at the European Commission to cybercrime group TeamPCP, which exploited a supply chain attack on the open-source security tool Trivy to steal 92 GB of compressed data from the Commission's AWS infrastructure. The notorious ShinyHunters gang then published the data, which included emails and personal details from up to 71 clients across EU institutions. The breach exposes the fragility of the open-source software supply chain that underpins the security tools governments rely on.

The European Union's computer emergency response team said on Thursday that a supply chain attack on an open-source security scanner gave hackers the keys to the European Commission's cloud infrastructure, resulting in the theft and public leak of approximately 92 gigabytes of compressed data including the personal information and email contents of staff across dozens of EU institutions.

CERT-EU attributed the breach to TeamPCP, a cybercrime group that has spent the past six weeks systematically compromising the very tools organisations use to defend themselves. The data was subsequently published online by ShinyHunters, the notorious extortion gang responsible for breaches at Ticketmaster, AT&T, and more than 60 other companies. The dual attribution, one group for the hack, another for the leak, is unusual in cybercrime investigations and suggests a growing ecosystem of specialisation among criminal operators.

The attack began on 19 March when the European Commission unknowingly downloaded a compromised version of Trivy, a widely used open-source vulnerability scanner maintained by Aqua Security. TeamPCP had exploited an incomplete credential rotation following an earlier breach of Trivy's GitHub repository in late February, retaining residual access to force-push malicious code to 76 of 77 version tags in the trivy-action repository. When the Commission's automated security pipeline pulled the poisoned update, the malware harvested an AWS API key that gave the attackers access to the Commission's cloud account on Amazon Web Services.

and an abnormal increase in network traffic. The Commission publicly disclosed the incident on 27 March. One day later, ShinyHunters published the dataset on their dark web leak site.

The scale of exposure is substantial. The stolen data relates to websites hosted for up to 71 clients of the Europa.eu web hosting service: 42 internal European Commission clients and at least 29 other EU entities. CERT-EU confirmed the published dataset, approximately 340 GB uncompressed, contained nearly 52,000 files of outbound email communications, along with lists of names, usernames, and email addresses. Agencies potentially affected include the European Medicines Agency, the European Banking Authority, ENISA itself, and Frontex, the EU's border and coast guard agency.

The Trivy compromise was not an isolated incident. Between 19 and 27 March, TeamPCP conducted what Palo Alto Networks called a systematic campaign against open-source security infrastructure. After Trivy, the group targeted Checkmarx KICS, an infrastructure-as-code scanner, force-pushing malicious commits to all 35 version tags on 21 March. They then pivoted to LiteLLM, an AI gateway tool, because BerriAI's CI/CD pipeline used Trivy for scanning, and the poisoned trivy-action harvested a PyPI publishing token that allowed the attackers to push malicious packages directly to the Python Package Index. Each compromised tool became a vector for reaching the next target, creating a cascading supply chain attack that affected organisations far beyond the European Commission.

The implications for the governance frameworks Europe has spent years building are uncomfortable. The EU's Cybersecurity Regulation, adopted in 2023, was designed to ensure institutional resilience against precisely this kind of attack. The NIS2 Directive holds board-level executives directly accountable for cybersecurity failures, with penalties including fines and disqualification. Yet the Commission's own infrastructure was compromised through a vector, a poisoned update to a security scanning tool, that falls squarely in the blind spot between supply chain management and runtime protection.

TeamPCP, also tracked as DeadCatx3, PCPcat, and ShellForce, has been documented by CrowdStrike, Wiz, and SANS as a cloud-native threat actor that exploits misconfigured Docker APIs, Kubernetes clusters, and Redis servers. The group has been linked to ransomware, data exfiltration, and cryptomining campaigns, and recently announced a partnership with CipherForce, another ransomware group, to co-publish breach data. The professionalisaton of cybercriminal operations, where specialists in initial access, lateral movement, and data extortion collaborate across organisational boundaries, mirrors the division of labour that makes legitimate cybersecurity companies scale rapidly.

ShinyHunters, for its part, is a known quantity. The syndicate has been operating since 2020 and owns Breach Forums, one of the dark web's most active marketplaces for stolen data. French national Sebastien Raoult was sentenced to three years in prison in Seattle for his role in the group's earlier operations, but the organisation has continued to operate. Its involvement in publishing the Commission's data suggests either a direct relationship with TeamPCP or a marketplace dynamic in which stolen data finds its way to the most effective distributor.

The breach arrives at a particularly sensitive moment for EU digital sovereignty. The Commission relies on AWS for parts of its web infrastructure, a dependency that has drawn scrutiny from European legislators who argue that critical government systems should run on European cloud providers. A breach that traces from a compromised open-source tool to an American cloud platform to a dark web leak site operated by an international criminal syndicate will do nothing to quiet those concerns. It will, however, intensify the debate about whether the EU's regulatory ambitions are matched by the operational security of its own institutions.

For the broader technology industry, the lesson is more immediate. The open-source security tools that organisations use to scan their code, audit their infrastructure, and validate their compliance, the tools that are supposed to be the last line of defence, have become the attack surface. Trivy alone is used by thousands of organisations worldwide. When the scanner becomes the weapon, the entire model of automated security breaks down, and the trust assumptions underpinning modern software infrastructure collapse with it.

CERT-EU is coordinating the incident response under the EU's Cybersecurity Regulation and continues to analyse the published dataset. For the 71 clients whose data may have been compromised, the remediation process is only beginning. For the European technology ecosystem that relies on the same open-source tools and cloud infrastructure, the breach is a warning that has already arrived too late.

Also tagged with

SECURITY

Published April 4, 2026 - 1:45 pm UTC

Back to top

Popular articles