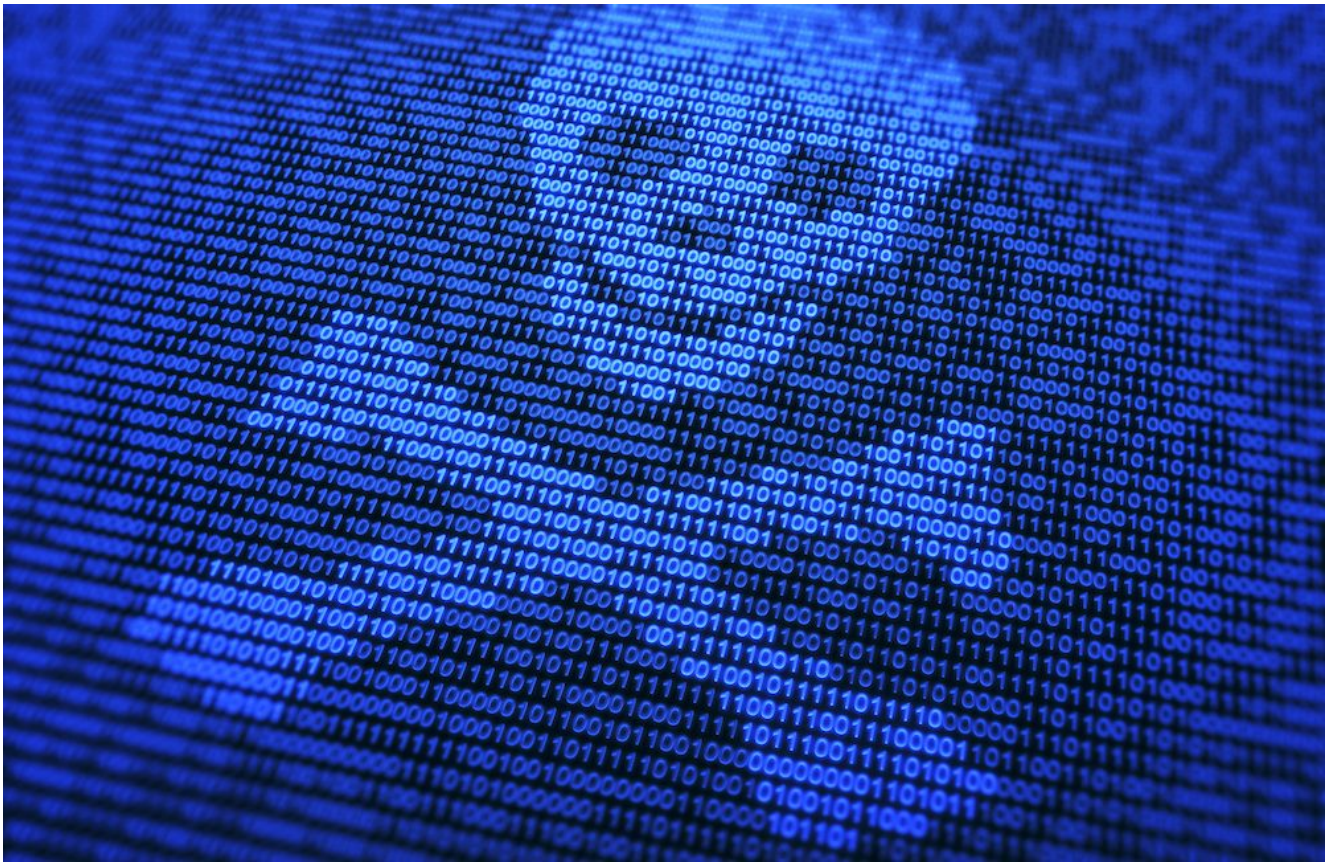
Widely used Trivy scanner compromised in ongoing supply-chain attack



Hackers have compromised virtually all versions of Aqua Security's widely used Trivy vulnerability scanner in an ongoing supply chain attack that could have wide-ranging consequences for developers and the organizations that use them.

Trivy maintainer Itay Shakury confirmed the compromise on Friday, following rumors and a thread, since deleted by the attackers, discussing the incident. The attack began in the early hours of Thursday. When it was done, the threat actor had used stolen credentials to force-push all but one of the trivy-action tags and seven setup-trivy tags to use malicious dependencies.

Assume your pipelines are compromised

A forced push is a git command that overrides a default safety mechanism that protects against overwriting existing commits. Trivy is a vulnerability scanner that developers use to detect vulnerabilities and inadvertently hardcoded authentication secrets in pipelines for developing and deploying software updates. The scanner has 33,200 stars on GitHub, a high rating that indicates it’s used widely.

“If you suspect you were running a compromised version, treat all pipeline secrets as compromised and rotate immediately,” Shakury wrote.

Security firms Socket and Wiz said that the malware, triggered in 75 compromised trivy-action tags, causes custom malware to thoroughly scour development pipelines, including developer machines, for GitHub tokens, cloud credentials, SSH keys, Kubernetes tokens, and whatever other secrets may live there. Once found, the malware encrypts the data and sends it to an attacker-controlled server.

The end result, Socket said, is that any CI/CD pipeline using software that references compromised version tags executes code as soon as the Trivy scan is run. Spoofed version tags include the widely used @0.34.2, @0.33, and @0.18.0. Version @0.35.0 appears to be the only one unaffected.

https://arstechnica.com/security/2026/03/widely-used-trivy-scanner-compromised-in-ongoing-supply-chain-attack/