Large enterprises scramble after supply-chain attack spills their secrets

Open source software used by more than 23,000 organizations, some of them in large enterprises, was compromised with credential-stealing code after attackers gained unauthorized access to a maintainer account, in the latest open source supply-chain attack to roil the Internet.

The corrupted package, tj-actions/changed-files, is part of tj-actions, a collection of files that's used by more than 23,000 organizations. Tj-actions is one of many GitHub Actions, a form of platform for streamlining software available on the open source developer platform. Actions are a core means of implementing what's known as CI/CD, short for Continuous Integration and Continuous Deployment (or Continuous Delivery).

Scraping server memory at scale

On Friday or earlier, the source code for all versions of tj-actions/changed-files received unauthorized updates that changed the "tags" developers use to reference specific code versions. The tags pointed to a publicly available file that copies the internal memory of severs running it, searches for credentials, and writes them to a log. In the aftermath, many publicly accessible repositories running tj-actions ended up displaying their most sensitive credentials in logs anyone could view.

"The scary part of actions is that they can often modify the

source code of the repository that is using them and access any secret variables associated with a workflow," HD Moore, founder and CEO of runZero and an expert in open source security, said in an interview. "The most paranoid use of actions is to audit all of the source code, then pin the specific commit hash instead of the tag into the … the workflow, but this is a hassle."

https://arstechnica.com/information-technology/2025/03/supply-chain-attack-exposing-credentials-affects-23k-users-of-tj-actions/