

Five OVHcloud CLI releases on GitHub replaced with secret-stealing build



On 19 October an attacker used a hijacked contributor account to swap the archives of five OVHcloud CLI releases on GitHub for a build that steals secrets from disk. The files were live for up to 94 minutes.

- The attacker took over a contributor's GitHub account and replaced the download archives of five existing OVHcloud CLI releases.
- The substituted build is designed to steal secrets stored on the disk of any machine that runs it.
- The malicious files were available from 12:47 to 14:21 UTC on Monday, 19 October, up to 94 minutes.
- The details come from OVHcloud's account as reported by The Hacker News.

What happened

According to OVHcloud, as reported by The Hacker News, an attacker gained control of a contributor's GitHub account on Monday, 19 October. Rather than publishing a new version, the attacker replaced the download archives attached to five existing releases of the OVHcloud command-line tool.

The replacement files were a build designed to steal secrets held on the disk of any machine that runs it. They were available on GitHub for up to 94 minutes, between 12:47 and 14:21 UTC.

Why it matters

Because existing release files were altered, a version number that looked familiar and trusted was no longer proof of a clean download. Command-line tools of this kind often run on administrator workstations and build servers, where credentials, tokens and keys are commonly stored. The source does not say how many users downloaded the files or whether any secrets were actually taken.

What to do next

Organisations that use the OVHcloud CLI should check whether anyone downloaded or updated it during the exposure window. Where a download did occur, treat the machine as potentially exposed and rotate the secrets it held. The steps below set out a practical order of work.

What to do now

1. Identify any download or update of the OVHcloud CLI from GitHub on 19 October between 12:47 and 14:21 UTC, using proxy, endpoint and CI logs.
2. Treat any machine that ran a build from that window as potentially compromised, isolate it and rotate the credentials, tokens and keys stored on it.
3. Review cloud account activity for the affected credentials for unexpected access.
4. Reinstall the tool only from a version confirmed clean by OVHcloud's guidance.
5. Record the event under your third-party and supply-chain risk process and brief your security leadership.