

OVHcloud CLI versions 0.11.0 to 0.15.0 backdoored via hijacked GitHub account



OVHcloud says attackers used a hijacked developer GitHub account to publish trojanized CLI releases 0.11.0–0.15.0 that steal secrets from disk. Anyone who ran them should clean the system and revoke all secrets.

- Versions 0.11.0 through 0.15.0 of the OVHcloud CLI were modified; 0.10.0 and 0.16.0 are clean.
- The malicious release appeared at 14:47 on October 19 and was blocked at 16:21 after a customer report.
- GitHub release immutability was disabled, so a privileged account could alter existing releases without passing CI/CD checks.
- OpenSourceMalware links the activity to GlassWorm; affected platforms are macOS, Linux and Windows, while source builds and Docker images were not affected.

- Anyone who ran an affected binary should treat all secrets on that machine as compromised.

OVHcloud has warned users that its open-source command-line tool, used by administrators and developers to manage cloud and hosting services and automate tasks, was tampered with to distribute information-stealing malware. According to the company's CEO, Octave Klabba, an attacker took over a developer's GitHub account, gained access to the CLI repository and modified versions 0.11.0 through 0.15.0.

What happened

The compromised release appeared at 14:47 on October 19 and was detected and blocked at 16:21 after a customer reported it. Version 0.10.0 and the latest 0.16.0 are clean. Klabba described the malware as poorly made, but its aim was to retrieve secrets from the disk.

OVHcloud later explained that GitHub's release immutability setting had been disabled. That allowed an account with sufficient privileges to change existing releases without passing CI/CD checks. The company says its pipelines, including tests and CVE detection, were not affected. It has since enabled the setting and considers the incident resolved.

Wider context

OpenSourceMalware, a community threat intelligence platform, believes the attack was likely part of a new GlassWorm operation. Its researchers say the pipelines were not tampered with and that the infected packages were built locally. They also report that the GitHub account had been compromised for more than six months. They did not analyze the payload itself. Affected platforms are macOS (Intel and ARM), Linux (x86_64 and ARM64) and Windows x86-64; source builds and Docker images were not affected.

What to do

Organizations using the tool should check which version they installed and when. Anyone who ran an affected binary should clean the system and revoke every secret stored on it, as the vendor advises.

What to do now

1. Inventory workstations, build servers and jump hosts running OVHcloud CLI and identify any that installed versions 0.11.0 to 0.15.0.
2. Update to 0.16.0 or remove the tool on affected machines; versions 0.10.0 and source or Docker builds were not affected.
3. For any machine that ran an affected binary, clean the system and revoke and rotate all secrets on its disk, including API keys, tokens and SSH keys.
4. Review OVHcloud account activity for the credentials involved and watch for unexpected use.
5. Enable release immutability and enforce MFA and least privilege on GitHub accounts and repositories your

teams maintain.

6. Record the event in your third-party and supply-chain risk register and follow your incident reporting procedures if secrets were exposed.