GL.iNet GoodCloud compromised: malware pushed to routers and KVMs



Attackers compromised GL.iNet's GoodCloud management service and installed malware on connected routers and KVMs. The cloud flaw is fixed, but devices stay infected until firmware is updated and checked.

- GL.iNet found on November 20, 2026 that GoodCloud was compromised through a cloud vulnerability it has not detailed; the flaw is now fixed.
- The cloud-side fix does not clean infected devices; the latest stable firmware removes that specific malware without a factory reset.
- The scope is still unknown, including whether computers attached to infected KVMs were affected.
- Partner RemoteToHome Consulting reported that 166 of 199 routers it reached showed the 20 November attack, an older backdoor, or both.

> - Attackers had root access in some cases, so keys, passwords and profiles on the device may have been copied.

Attackers compromised GoodCloud, the cloud remote management service run by GL.iNet, and used it to install malware on routers and KVM devices connected to it. GL.iNet is still investigating and has not said how many devices are affected.

What GL.iNet has said

The company found the compromise on November 20, 2026, and says the underlying cloud vulnerability, which it has not described, has been fixed. That fix does not clean devices already infected. GL.iNet advises installing the latest stable security firmware, which removes that specific malware and does not require a factory reset.

Its published indicator is a process running as crond -i /tmp/.log. The company later added that other indicators exist which its official quick checks do not surface, and it pointed to a community script for extra detection and clean-up. It cautions that neither approach can guarantee a device is clean. For infected KVMs, the connected computer should be checked for unfamiliar programs, browser extensions, user accounts, startup items, scheduled tasks and unusual network activity.

Findings from a partner

RemoteToHome Consulting, a GL.iNet services partner, checked routers it manages. Of 199 reached, 166 showed the 20 November attack, an older backdoor, or both. It could not determine how the older backdoors arrived. It also published an analysis of a command injection flaw in the GoodCloud client that it believes was used; GL.iNet has not confirmed this.

Because the attacker had a root shell, RTH warns that stored keys, passwords and profiles could have been copied, and that reinstalling the router does not undo this. Access must be revoked at the other end.

What to do now

1. Inventory GL.iNet routers and KVMs in use, including any enrolled in GoodCloud, across offices, branches and remote staff.
2. Install the latest stable GL.iNet firmware on affected devices and run both GL.iNet's checks and the RTH indicator list.
3. Treat any confirmed device as exposed: rotate keys, passwords and VPN credentials stored on it, and revoke access elsewhere.
4. Inspect computers attached to infected KVMs for unfamiliar programs, accounts, scheduled tasks and network activity.
5. Disable cloud remote management on these devices where it is not essential, and follow your incident-

reporting duties to NCA or SAMA if a compromise is confirmed.