Zyxel GS1900 switches: earlier patch does not stop exploited flaw; new firmware released



Binarly found that Zyxel GS1900 switches with the earlier fix remain exposed to an actively used exploit. Zyxel has issued new firmware for 10 GS1900 models.

- Binarly researchers found the earlier Zyxel fix does not block the exploit attackers used.
- The flaw lets anyone who can reach the web management interface run commands without logging in.
- The flaw has been exploited in active attacks.
- Zyxel released new firmware for 10 GS1900 models that closes the hole.
- The earlier fix is described in the source as version 2.90.

What was found

Researchers at Binarly report that Zyxel GS1900 network switches which received the vendor's earlier fix for an actively exploited flaw can still be attacked with the same exploit. The earlier fix is identified in the source as 2.90. In practice, a switch that was patched and marked as remediated may still be vulnerable.

The flaw allows anyone who can reach a switch's web management interface to run commands on the device without authenticating. Because the issue is already being exploited, exposure of that interface is the main concern.

What Zyxel has done

Zyxel has released new firmware for 10 GS1900 models that closes the hole. The source excerpt does not list the affected models, the new version numbers or a CVE identifier, so teams should take those details from the vendor's own advisory.

Why it matters

Network switches sit at the core of internal connectivity, and a compromised device can give an attacker a foothold inside the network. Institutions that closed this item after applying the earlier update should reopen it and verify the firmware actually installed.

What to do now

1. Inventory all Zyxel GS1900 switches and confirm model and installed firmware version.
2. Treat devices updated only with the earlier fix as still vulnerable and reopen the remediation ticket.
3. Apply the new Zyxel firmware to affected models after testing, following change control.
4. Restrict the web management interface to a dedicated management network and block access from user and internet-facing segments.
5. Review switch logs and configurations for unexpected commands or changes, and escalate any findings through incident procedures.