# D-Link issues mitigation guidance for unpatched flaws in DGS-3130 switches



D-Link has shared mitigation measures for multiple unpatched security flaws affecting its DGS-3130 series managed Gigabit stackable switches. Operators should review the vendor's guidance.

- D-Link has published mitigation measures for its DGS-3130 series.
- The affected products are managed Gigabit stackable switches.
- The flaws are described as multiple and unpatched, so mitigation is the available response.
- The source excerpt does not give CVE numbers, technical details or patch timelines.

## What was announced

D-Link has shared mitigation measures for multiple security flaws affecting the DGS-3130 series of managed Gigabit stackable switches. According to the report, these flaws do not yet have patches, which is why the vendor is pointing customers to interim measures.

## What is not yet known

The excerpt available to us does not list CVE identifiers, the technical nature of the flaws, affected firmware versions or a date for fixes. We therefore avoid drawing conclusions about severity or exploitation beyond what the vendor has said. Teams should read the original vendor guidance directly before acting.

## What to do next

Institutions that use these switches in branch, data centre or campus networks should first confirm whether any DGS-3130 units are deployed, including in stacks and in less visible locations. Once identified, apply the vendor's mitigation measures and limit who can reach the management interfaces of these devices. Monitor the vendor's advisory page for firmware updates and plan a change window so a patch can be applied quickly once released.

Where network devices support critical services, record the exposure in the risk register, with an owner and a review date, until a fix is installed.

## What to do now

1. Inventory all DGS-3130 series switches, including stacked units and remote sites.
2. Read the vendor's mitigation guidance and apply it to each affected switch.
3. Restrict access to switch management interfaces to a dedicated administration network or named hosts.
4. Monitor the D-Link advisory page and prepare a change window for firmware updates once available.
5. Record the unpatched exposure in the risk register with an owner and review date.