

Zyxel GS1900 Series Switches Vulnerable to Stack-Based Buffer Overflow



A stack-based buffer overflow vulnerability in Zyxel GS1900 series switches allows unauthenticated attackers on the local network to execute operating system commands through crafted HTTP requests.

- CVE-2026-7273 affects Zyxel GS1900 series switches through a stack-based buffer overflow in the CGI program
- Unauthenticated attackers on the local network can exploit the flaw via crafted HTTP requests
- Successful exploitation may allow arbitrary operating system command execution
- Organisations must apply vendor patches or discontinue use if mitigations are unavailable
- Asset owners should evaluate internet exposure and prioritise patching based on risk

Vulnerability Overview

Zyxel GS1900 series network switches contain a **stack-based buffer overflow vulnerability** tracked as CVE-2026-7273. The flaw resides in the CGI program component of affected devices and can be exploited by an unauthenticated attacker with access to the local area network. By sending a specially crafted HTTP request to a vulnerable switch, an attacker may trigger the buffer overflow condition and potentially execute arbitrary operating system commands on the device.

The vulnerability does not require authentication, lowering the barrier to exploitation for threat actors who have gained a foothold on the internal network. This makes the flaw particularly concerning for organisations where network switches are deployed in environments with limited network segmentation or where insider threats are a consideration.

Risk to Saudi Institutions

Regulated institutions in the Kingdom that deploy Zyxel GS1900 series switches in their network infrastructure face operational and compliance risks. Successful exploitation could compromise network integrity, enable lateral movement within the environment, or facilitate data exfiltration. Organisations subject to the National Cybersecurity Authority's Essential Cybersecurity Controls or SAMA Cyber Security Framework should treat this vulnerability as a priority patching matter.

Asset owners must evaluate whether affected switches are exposed to untrusted network segments or the internet, and assess the potential impact on critical systems and data flows.

Recommended Response

Organisations should immediately identify all Zyxel GS1900 series switches in their environment and apply vendor-supplied patches or mitigations without delay. If patches are not available or cannot be applied promptly, consider isolating affected devices or discontinuing their use until remediation is possible. Network segmentation and access controls should be reviewed to limit exposure of management interfaces to trusted administrators only.

What to do now

1. Identify all Zyxel GS1900 series switches deployed in your network infrastructure
2. Apply vendor-supplied security patches or mitigations immediately upon availability
3. Evaluate internet and untrusted network exposure of affected switches and isolate where necessary
4. Review network segmentation to ensure management interfaces are accessible only to authorised administrators
5. Discontinue use of affected devices if patches are unavailable and risk cannot be mitigated
6. Document remediation actions and timelines for compliance reporting to NCA or SAMA as applicable