Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Zyxel GS1900 Switches Under Active Attack

Date of Publication	Admiralty Code	TA Number
September 23, 2026	A1	TA2026277

Summary

First Seen: June 2026
Affected Products: Zyxel GS1900 Series Smart Managed Switches (GS1900-8, GS1900-8HP, GS1900-10HP, GS1900-16, GS1900-24, GS1900-24E, GS1900-24EP, GS1900-24HPv2, GS1900-48, GS1900-48HPv2)
Impact: CVE-2026-7273 is a stack-based buffer overflow in the CGI (web management) component of Zyxel GS1900 series smart managed switches. A LAN-based attacker who has not logged in can send a specially crafted HTTP request to the device and run operating-system commands on it. Zyxel released fixed firmware in June 2026, but a threat actor began exploiting switches that had not been patched, with activity tied to this flaw starting on or about August 17, 2026. The actor compromised and stole data from 996 GS1900 switches across 48 countries. Patched firmware is available, so organizations running affected GS1900 switches should update to the fixed version immediately and check their devices for signs of compromise.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-7273	Zyxel GS1900 Series Switches Stack-Based Buffer Overflow Vulnerability	Zyxel GS1900 Series Switches	✗	✓	✓

Vulnerability Details

#1

CVE-2026-7273 is a stack-based buffer overflow (CWE-121) in the CGI program that powers the web management interface of Zyxel GS1900 series switch firmware. A buffer overflow happens when a program accepts more input than the memory space it set aside can hold, so the extra data spills into adjacent memory. When an attacker controls that overflow, they can corrupt how the program runs and ultimately steer it into executing their own commands.

#2

Exploitation needs no credentials. An attacker on the same local network sends a crafted HTTP request to the switch's management interface, and a successful request lets them execute operating-system commands on the device. Because the flaw is reached before any login, and the switch is a trusted piece of network plumbing, a single request can turn a managed switch into an attacker-controlled one.

#3

The vulnerability affects GS1900 firmware version 2.90(XXXX.1)C0 and earlier across ten models, and Zyxel published patched firmware for the supported models on June 16, 2026. The exploit observed in the wild was written specifically for firmware 2.10 through 2.90 of the GS1900-24. Still, it included options that let the attacker adapt it to other affected models and firmware, so every unpatched GS1900 in scope should be treated as at risk.

#4

The actor carried out the exploitation using a Python script hidden with the commercial obfuscation tool PyArmor (a legacy 6.7.5 runtime was left in place, which aided analysis). After breaking into a switch, the actor used the exploit to fetch a small custom collector script over TFTP from its own infrastructure, ran it to gather the device's configuration, hashed root credentials, and network details, and staged that data on the device for retrieval. GreyNoise reported that 996 switches across 48 countries were compromised, led by Italy, the United States, Taiwan, France, and South Korea, and that 564 of them were still using factory-default credentials. The takeaway is straightforward: Zyxel's patched firmware closes this flaw, so any GS1900 switch still on a vulnerable version should be updated without delay.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-7273	Zyxel GS1900-8 (Before 2.90(AAHH.2)C0), GS1900-8HP (Before 2.90(AAHI.2)C0), GS1900-10HP (Before 2.90(AAZI.2)C0), GS1900-16 (Before 2.90(AAHJ.2)C0), GS1900-24 (Before 2.90(AAHL.2)C0), GS1900-24E (Before 2.90(AAHK.2)C0), GS1900-24EP (Before 2.90(ABTO.2)C0), GS1900-24HPv2 (Before 2.90(ABTP.2)C0), GS1900-48 (Before 2.90(AAHN.2)C0), GS1900-48HPv2 (Before 2.90(ABTQ.2)C0)	cpe:2.3:o:zyxel:gs1900-8_firmware:*:*:*:*:*:*:*:*, cpe:2.3:o:zyxel:gs1900-8hp_firmware:*:*:*:*:*:*:*:*, cpe:2.3:o:zyxel:gs1900-10hp_firmware:*:*:*:*:*:*:*:*, cpe:2.3:o:zyxel:gs1900-16_firmware:*:*:*:*:*:*:*:*, cpe:2.3:o:zyxel:gs1900-24_firmware:*:*:*:*:*:*:*:*, cpe:2.3:o:zyxel:gs1900-24e_firmware:*:*:*:*:*:*:*:*, cpe:2.3:o:zyxel:gs1900-24ep_firmware:*:*:*:*:*:*:*:*, cpe:2.3:o:zyxel:gs1900-24hpv2_firmware:*:*:*:*:*:*:*:*, cpe:2.3:o:zyxel:gs1900-48_firmware:*:*:*:*:*:*:*:*, cpe:2.3:o:zyxel:gs1900-48hpv2_firmware:*:*:*:*:*:*:*:*	CWE-121

Recommendations

Update the Firmware Now: Install Zyxel's patched firmware for your GS1900 model without delay (for example, 2.90(AAHL.2)C0 for the GS1900-24). Patching is the direct fix for this flaw, and every unpatched switch on your network remains open to unauthenticated command execution. If a patch is not available for a device, CISA advises discontinuing its use.

Replace Default and Weak Credentials: More than half of the compromised switches were still using factory-default logins. Change every default and reused password on your GS1900 devices to strong, unique credentials, and confirm no device is reachable with out-of-the-box settings.

Restrict the Management Interface: Limit access to the switch web/CGI management interface to a trusted administrative network or VLAN, and make sure these devices are not exposed to untrusted or internet-facing segments. This shrinks the pool of hosts that could send the malicious request.

Watch for Attacker Behavior on the Switch: Alert on and block unexpected outbound TFTP transfers from switch management interfaces to external hosts, and check devices for the collector script and its staged output file (/home/web/tmp/info.txt). Because GreyNoise withheld the exploitation IP address, these host- and network-level behaviors are the most reliable signals for this activity.

Vulnerability Management: Maintain an up-to-date inventory of network devices and their firmware versions so security updates can be applied quickly when vendors release them. Prioritize internet-adjacent and infrastructure devices such as switches, routers, and firewalls, which give attackers broad visibility and control once compromised.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1587: Develop Capabilities	T1587.001: Malware
	T1608: Stage Capabilities	T1608.001: Upload Malware
	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.006: Python
Defense Evasion	T1027: Obfuscated Files or Information	T1027.002: Software Packing
Command and Control	T1105: Ingress Tool Transfer	
Collection	T1119: Automated Collection	
	T1005: Data from Local System	

Patch Link

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026

References

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026

https://www.greynoise.io/blog/open-season-on-kapibala-attacker-steals-government-records-wordpress-exploitation

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 23, 2026 • 01:50 AM

More at www.hivepro.com