D-Link WiFi Extender contains vulnerabilities that are vulnerable to malicious attacks

With the identifier CVE-2023-45208, this vulnerability was first discovered by a group of security researchers from the RedTeam team.

D-Link DAP-X1860 WiFi 6, one of the most commonly used WiFi Extender models on the market today, is said to contain serious vulnerabilities, making them vulnerable to DoS (denial of service) attacks. service) and remote command injection. The product is still widely available for sale by D-Link and has thousands of reviews on Amazon.

WiFi Extender is a type of WiFi booster that extends your main router's internet signal to another location. It connects to the home network via Ethernet or coaxial cable. Essentially, WiFi Extenders work on the model of adding another router to any WiFi 'dead zones' or areas in your home that don't receive an internet signal.

With the identifier CVE-2023-45208, this vulnerability was first discovered by a group of security researchers from the RedTeam team. They tried to warn D-Link many times, but the company remained silent and no fix has been released as of now.

The problem lies in the network scanning function of the D-Link DAP-X1860. Specifically, the device is not capable of parsing SSIDs that contain a check mark (') in the name, misinterpreting it as the end of a command.

Technically, the problem stems from the 'parsing_xml_stasurvey' function in the libcgifunc.so library, which contains a system command to execute.

However, because the product lacks an SSID scanning feature, attackers can easily abuse this for malicious purposes. Within the scope of the extender, it is possible for a hacker to set up a WiFi network and give it the same phishing name that the victim usually uses, but include a check mark in the name, such as 'TipsMake's Network,'. When the device tries to connect to that SSID, this action will generate the error "Error 500: Internal Server Error".

If an attacker adds a second part to the SSID containing a shell command separated by "&&" like "Test' && uname -a &&", the extender will be tricked into executing the 'uname -a' command when setting Network setup/scanning.

All processes on the extender, including any commands injected by an external threat actor, run as root, potentially allowing an attacker to probe other devices connected to the extender expand and continue to infiltrate their network.

The most difficult prerequisite for the attack is forcing a network scan on the target device, but this can be overcome by performing a deauthentication attack.

Several available software tools can generate and send authentication packets to the extender, causing it to disconnect from the main network and forcing the target to perform a network scan.

RedTeam researchers discovered this vulnerability in May 2023 and reported it to D-Link. But so far, the group has not received any response. This means that the D-Link DAP-X1860 is currently still vulnerable, and the relatively simple exploit mechanism makes the situation dangerous.

Owners of the D-Link DAP-X1860 extender should limit manual network scanning, handle suspicious disconnections, and turn off the extender when not in regular use.

Additionally, consider installing IoT devices and range extenders on a separate network, especially for sensitive devices containing personal or work data.