VULNERABILITIES

Newly Disclosed Vulnerability Exposes EOL Arris Routers to Attacks

Malwarebytes warns of a remote code execution vulnerability impacting Arris G2482A, TG2492, and SBG10 routers, which have reached end-of-life (EOL).

By Ionut Arghire
February 17, 2023

Malwarebytes warns of a remote code execution vulnerability impacting several Arris routers, for which proof-of-concept (PoC) exploit code has been released.

TRENDING

1 Atlassian Investigating Security Breach After Hackers Leak Data

2 SolarWinds Announces Upcoming Patches for High-Severity Vulnerabilities

3 Firefox Updates Patch 10 High-Severity Vulnerabilities

Tracked as CVE-2022-45701, the bug exists because the router firmware does not properly neutralize special characters in requests, which allowed security researcher Yerodin Richards to perform shell script command injection.

The impacted models have reached end-of-life (EOL) and are no longer supported by CommScope (the company that acquired Arris), meaning that they are unlikely to receive patches.

The security defect impacts G2482A, TG2492, and SBG10 routers running firmware version 9.1.103, which are commonly found in the Latin America and Caribbean region.

Although login credentials are required to exploit the vulnerability, users often leave default usernames and passwords on their devices, either because the process of changing or removing them is too complicated or because they are not explicitly told to modify them during the setup process.

Not only are these routers susceptible to attacks that rely on brute-forcing default credentials, but, because they do not secure

4 Apple Patches Actively Exploited WebKit Zero-Day Vulnerability

5 Patch Tuesday: Microsoft Warns of Exploited Windows Zero-Days

6 'Frebniis' Malware Hijacks Microsoft IIS Function to Deploy Backdoor

7 Spanish, US Authorities Dismantle Cybercrime Ring That Defrauded Victims of $5.3 Million

8 Hackers Earn $180,000 for ICS Exploits at Pwn2Own Miami 2023

credentials in transit using HTTPS, they are also prone to exposing them to attackers able to intercept traffic.

To mitigate the risks, users are advised to secure their devices with strong passwords, albeit an experienced attacker able to eavesdrop on the unprotected traffic could intercept the password.

Changing the router firmware would be a better solution, but "providers are lax about pushing updates and there is no easy way for an end user to do this themselves," Richards says.

According to the security researcher, users "could run the exploit to gain a root shell and try to patch it from there but this is by no means a simple solution".

Related: Remote Code Execution Vulnerabilities Found in TP-Link, NetComm Routers

Related: InHand Industrial Router Vulnerabilities Expose Internal OT Networks to Attacks

Related: Cisco Warns of Critical Vulnerability in EoL Small Business Routers