Issued 9/7/17

Router Flaws Put AT&T Customers at Hacking Risk

Thousands of routers, many of which belong to AT&T U-verse customers, can be easily and remotely hacked through several critical security vulnerabilities.

Five flaws were found in common consumer Arris routers, used by AT&T customers and other internet providers around the world. The flaws were detailed in a blog post by Joseph Hutchins, who described some of the flaws as being as a result of "pure carelessness."

Among the vulnerabilities are hardcoded credentials, which can allow "root" remote access to an affected device, giving an attacker full control over the router. An attacker can connect to an affected router and log-in with a publicly-disclosed username and password, granting access to the modem's menu-driven shell. An attacker can view and change the Wi-Fi router name and password, and alter the network's setup, such as rerouting internet traffic to a malicious server.

The shell also allows the attacker to control a module that's dedicated to injecting advertisements into unencrypted web traffic, a common tactic used by internet providers and other web companies. Hutchins said that there was "no clear evidence" to suggest the module was running but noted

that it was still vulnerable, allowing an attacker to inject their own money-making ad campaigns or malware.

Buggy routers don't always lead to unauthorized network access, but can instead be hijacked as part of botnet operations, like Mirai, which when powered up can target and throw websites and services offline.