Issued 4/30/18

Critical Vulnerability Found In over a Million GPON Home Routers

The researchers have found a way to bypass the authentication to access the GPON home routers (CVE-2018-10561). The experts chained this authentication bypass flaw with another command injection vulnerability (CVE-2018-10562) and were able to execute commands on the device.

Analyzing the firmware of the GPON home routers, the experts found two different critical vulnerabilities (CVE-2018-10561 & CVE-2018-10562) that could be chained to allow complete control of the vulnerable device and therefore the network. The first vulnerability exploits the authentication mechanism of the device, it could be exploited by an attacker to bypass all authentication. The vulnerability effects the build in HTTP servers, which check for specific paths when authenticating. This allows the attacker to bypass authentication on any endpoint using a simple trick.