CVE-2019-16920 - Score: 9.8

Components:

dlink dir-655 firmware *
dlink dir-655 cx

Description:

Unauthenticated remote code execution occurs in D-Link products such as DIR-655C, DIR-866L, DIR-652, and DHP-1565. The issue occurs when the attacker sends an arbitrary input to a "PingTest" device common gateway interface that could lead to common injection. An attacker who successfully triggers the command injection could achieve full system compromise. Later, it was independently found that these are also affected: DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835, and DIR-825.

Main problems:

78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')"