# CVE Detail – CVE-2022-4390

A network misconfiguration is present in versions prior to 1.0.9.90 of the NETGEAR RAX30 AX2400 series of routers. IPv6 is enabled for the WAN interface by default on these devices. While there are firewall restrictions in place that define access restrictions for IPv4 traffic, these restrictions do not appear to be applied to the WAN interface for IPv6. This allows arbitrary access to any services running on the device that may be inadvertently listening via IPv6, such as the SSH and Telnet servers spawned on ports 22 and 23 by default. This misconfiguration could allow an attacker to interact with services only intended to be accessible by clients on the local network.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.28188

## CVSS Scoring

CVSS v3.1 Score: 10.0

Severity: CRITICAL

## Affected Products

* cpe:2.3:o:netgear:ax2400\_firmware:\*:\*:\*:\*:\*:\*:\*:\*