# CVE Detail – CVE-2021-22909

A vulnerability found in EdgeMAX EdgeRouter V2.0.9 and earlier could allow a malicious actor to execute a man-in-the-middle (MitM) attack during a firmware update. This vulnerability is fixed in EdgeMAX EdgeRouter V2.0.9-hotfix.1 and later.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.6527

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-295: Improper Certificate Validation
* CWE-300: Channel Accessible by Non-Endpoint

## CAPEC(s)

* CAPEC-459: Creating a Rogue Certification Authority Certificate
* CAPEC-466: Leveraging Active Adversary in the Middle Attacks to Bypass Same Origin Policy
* CAPEC-475: Signature Spoofing by Improper Validation
* CAPEC-57: Utilizing REST's Trust in the System Resource to Obtain Sensitive Data
* CAPEC-589: DNS Blocking
* CAPEC-590: IP Address Blocking
* CAPEC-612: WiFi MAC Address Tracking
* CAPEC-613: WiFi SSID Tracking
* CAPEC-615: Evil Twin Wi-Fi Attack
* CAPEC-662: Adversary in the Browser (AiTB)
* CAPEC-94: Adversary in the Middle (AiTM)

## ATT&CK Techniques

* T1557: Adversary-in-the-Middle
* T1040: Network Sniffing
* T1185: Browser Session Hijacking

## Used By (Actors/Tools)

* TrickBot (malware)
* cd00r (malware)
* JumbledPath (malware)
* VersaMem (malware)
* Ursnif (malware)
* J-magic (malware)
* Emotet (malware)
* TRANSLATEXT (malware)
* Regin (malware)
* Line Dancer (malware)
* IcedID (malware)
* Line Runner (malware)
* FoggyWeb (malware)
* Chaes (malware)
* Grandoreiro (malware)
* MESSAGETAP (malware)
* XLoader (malware)
* Cobalt Strike (malware)
* Carberp (malware)
* Penquin (malware)
* Melcoz (malware)
* Agent Tesla (malware)
* QakBot (malware)
* Dridex (malware)
* Dok (malware)
* NPPSPY (tool)
* Impacket (tool)
* Empire (tool)
* PoshC2 (tool)
* Responder (tool)
* NBTscan (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Sandworm Team (intrusion-set)
* APT28 (intrusion-set)
* Kimsuky (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* DarkVishnya (intrusion-set)
* Sea Turtle (intrusion-set)
* Salt Typhoon (intrusion-set)
* APT33 (intrusion-set)

## Affected Products

* cpe:2.3:o:ui:edgemax\_edgerouter\_firmware:\*:\*:\*:\*:\*:\*:\*:\*