Corero SmartWall® *Threat Advisory*

TP240PhoneHome DDoS reflection/amplification attack vector in the wild

Advisory ID: 03142022-1
Published: 14 March 2022

Summary

A Mitel vulnerability (CVE-2022-26143) in the TP-240 component of their *Micollab (before 9.4 SP1 FP1)* and *MiVoice Business Express (through 8.1)* products allows remote attackers to launch UDP reflection attacks with an amplification factor of 220 billion percent – triggered by a single packet.

The Corero SecureWatch DDoS Threat Intelligence team has observed an increase in this DDoS attack vector against customers over the recent days.

Threat Vector

This DDoS vector uses a reflective method in which an attacker makes a spoofed request, with a source IP address of the victim, to vulnerable servers on UDP port 10074, which then reply to the victim with a huge number (4,294,967,296) of response packets.

Recommended Action: SecureWatch Customers

TP240PhoneHome reflection/amplification attacks are exclusively from UDP source port 10074. This attack traffic is detected and safely mitigated by SmartWall's automatic zero-day Smart-Rule protection.

SmartWall DDoS protection solutions mitigate a wide range of known and zero-day attacks, all while maintaining the availability of applications and services being protected and without disrupting the delivery of legitimate traffic. They are designed to handle large DDoS floods, reflective amplified spoof attacks (such as TP240PhoneHome), as well as attacks that are typically too low, or short, to be mitigated manually, or by traditional out-of-band solutions.

Corero customers using the latest software releases and recommended SmartWall protection settings are comprehensively defended from this increase in DDoS activity.

Please contact Corero Support if you have any questions.