Dear Cisco Customer,

Cisco engineering has identified the following software issue with the release that you have selected that may affect your use of this software. Please review the Software Advisory notice here to determine if the issue applies to your environment.

Affected Software and Replacement Solution for CSCvq81354		
Software Type	**Software Affected**	**Software Solution**
Firepower Threat Defense (FTD) Software	**Version:** 6.4.0 – 6.4.0.5	**Version:** 6.4.0.7 or later

Reason for Advisory:

This software advisory addresses one software issue.

CSCvq81354
Firepower 1010 Series internal switch blackholes egress traffic on port-channel interfaces

Affected Platforms:
Firepower 1010 with FTD 6.4.0–6.4.0.5

Symptom:
Due to an internal traffic hashing issue, some EtherChannels on Firepower 1010 devices may blackhole some egress traffic. The hashing is based on source/destination IP address so the behavior will be consistent for a given source/destination IP pair. That is, some traffic consistently works and some consistently fails.

Conditions:
This only affects traffic that egresses an EtherChannel on a Firepower 1010 running FTD 6.4.0–6.4.0.5.

Workaround:
We strongly recommend you do not configure EtherChannels on Firepower 1010 devices running FTD Version 6.4.0, 6.4.0.3, 6.4.0.4, or 6.4.0.5. (Versions 6.4.0.1 and 6.4.0.2 are not supported on this model.)

Upgrade to FTD 6.4.0.7 or a later release.