Corero SmartWall® Threat Defense System
Threat Update Advisory

Advisory ID: 012017-1

Published: 20 January 2017

Summary

The Corero SecureWatch® Team has observed multiple confirmed instances of attacks using the Mirai botnet, for which the Corero SmartWall Threat Defense System already delivers proactive zero-day protection. Based on these observations, the SecureWatch team has developed a configuration change to the Smartwall policy which can be applied to further enhance mitigation of certain Mirai attack vectors.

Threat Vector

The Mirai GRE/IP flood vector has been found to utilize both random, or attacker-specified, inner-tunnel IP addresses and port numbers. The complexity of the attacks are further compounded by the size of the botnet being used, due to the number of unique outer-tunnel source IP addresses involved. Based on these observations, the SecureWatch team has identified additional protection opportunities via SmartWall flex-rule(s).

Recommended Action for SecureWatch Maintain Customers:

SmartWall already delivers proactive zero-day protection for the numerous Mirai attack vectors. SecureWatch Maintain customers, who suspect they are at risk from the Mirai GRE attack vector, can request details of the enhanced flex-rule protection from the SecureWatch team.

Recommended Action SecureWatch Managed Customers:

The SecureWatch team proactively tunes protection for SecureWatch Managed systems, so no customer action is required.