Corero SmartWall® Threat Defense System
Threat Advisory

Advisory ID: 022818-1
Published: 28 February 2018

Summary

Corero SecureWatch® Team has seen a rise in reflective Memcached attacks (Reflective UDP/11211) over the past week, for which the SmartWall® Solution already delivers proactive zero-day protection.

Threat Vector

This threat uses a reflective method in which the attacker makes a spoofed request (with a source IP address of the intended victim) to a Memcached server, which then replies to the victim with a large response. These attacks use UDP and will arrive at the victim from source port 11211 and are sometimes destined for a handful of destination ports but more often a single destination IP and port.

Recommended Action: SecureWatch Maintain Customers

The SmartWall solution has several methods to mitigate a reflective Memcached attack, using either the Smart-Rule or Flex-Rule capabilities:

Recommended: Smart-Rules

To block incoming attacks (source port 11211) using Smart-Rules, confirm the following rule settings:

1. Reflection Flood SmartRules cns-002031 and cns-002033 are set to Block Mode.
2. UDP Server flood SmartRules cns-002035 and cns-002037 are set to Block Mode.

Note: No additional threshold adjustments are recommended.

Optional: Flex-Rules

To block all incoming UDP Memcached responses from source port 11211, add the following Flex-Rule:

Name: Reflective_Res_Memcached
Filter Term: udp and src port 11211 and (len=1442 or len=1446) and udp[14:2]=0x0000

To block all incoming exploit attempts to UDP destination port 11211, which in turn will prevent outgoing attacks from your network, add the following Flex-Rule:

Name: Reflective_Req_Memcached
Filter Term: udp and dst port 11211 and udp[12:4]=0x00010000

Recommended Action: SecureWatch Managed Customers

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