corero
FIRST LINE OF DEFENSE

Corero SmartWall® Threat Update Advisory

Advisory ID: 102416-1

Published: 24 October 2016

Summary

The Corero SecureWatch® Team has seen a rise in reflective LDAP attacks over the past week. The SmartWall Solution has proactive protection for this type of attack vector with no intervention required from zero-day.

Threat Vector

This attack is a reflective CLDAP attack in which the attacker makes a spoofed request (with a source IP address of the intended victim) to an CLDAP server which then replies to the victim with a large response. This attack uses UDP and will arrive at the victim from source port 389 and often destined for a handful of destination ports. The UDP amplification on this attack ranges from 30x to 55x with the average being 46x.

Recommended Action SecureWatch Customers:

Confirm that SmartRule cns-002033 is set to Block Mode.

Confirm that SmartRule cns-002037 is set to Block Mode.

Confirm that the Fragments Smart Rule is set to enabled.

Recommended Action SecureWatchPlus Customers:

None – SmartWall solution has been tuned to proactively mitigate this type of attack vector.