corero
FIRST LINE OF DEFENSE

Corero SmartWall Threat Update Advisory

Advisory ID: 111516-1

Published: 16 November 2016

Summary

Corero SecureWatch Team has researched the recently disclosed BlackNurse DOS vector.

Corero SOC is able to monitor the presence of BlackNurse like packets on protected customers. The SmartWall Solution has proactive protection for this type of attack vector.

Threat Vector

This BlackNurse attack is based on unsolicited ICMP floods with Type 3 and Code 3 packets.

Recommended Action SecureWatch Maintain Customers:

If required, customer may create a generic Flex-Rule that will include the BlackNurse attack by adding the following filter.

Filter Term: icmp and icmp[0]=3 and icmp[1]=3

Recommended Action SecureWatch Managed Customers:

None – SecureWatch team proactively tuning systems.