Array Networks Security Advisory for CVE-2015-0235

Advisory Date: January 29, 2015

The purpose of this Array Networks Security Advisory is to advise customers that Array Networks products are not exposed to the CVE-2015-0235 vulnerability since we have an Array-proprietary Operating System.

Overview

Unlike other vendors who use the glibc library, Array Networks products are not exposed to the CVE-2015-0235 vulnerability since we have an Array proprietary Operating System.

Details

A heap-based buffer overflow, known as "GHOST", was found in glibc's__nss_hostname_digits_dots() of the glibc library. This bug can be remotely or locally triggered by the gethostbyname* functions. A remote attacker might exploit this flaw to execute arbitrary code to launch malicious attacks.

Array products, including APV, vAPV, AG, vxAG, TMX, and SPX products, use Array's proprietary Operating System. Therefore, services on Array products are not affected by this "GHOST" vulnerability.

Should you have any questions, please contact one of our customer service representatives at support@arraynetworks.com or Array Networks TAC telephone.