Array Networks Security Advisory: Bash Vulnerability CVE-2014-6271

Advisory Date: September 29, 2014

Vulnerability Overview

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock."

Impact

This vulnerability can allow unauthorized disclosure of information, unauthorized modification, and disruption of service.

Array Networks (APV, AG, WAN, SPX and TMX) do not expose bash for any kind of remote access such as SSH, WebUI, XML/RPC, or application portal, and therefore are not affected by the CVE 2014-6271 vulnerability.

Status

No Array products are affected by this vulnerability.

Mitigation

None required.

Array Networks Solution

No action required.