Array Networks Security Advisory:
Bash Vulnerability CVE-2014-6271, CVE-2014-6277 and CVE-2014-6278

Advisory Date: October 15, 2014

CVE-2014-6271Vulnerability 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."

CVE-2014-6277 Vulnerability Overview

GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access, and untrusted-pointer read and write operations) 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. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271 and CVE-2014-7169.

CVE-2014-6278 Vulnerability Overview

GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary commands 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. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277.

Impact

These vulnerabilities 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, CVE-2014-6277 or CVE-2014-6278 vulnerability.

Status

No Array products are affected by this vulnerability.

Mitigation

None required.

Array Networks Solution

No action required.