

Lund, Sweden Sep 26, 2014

CVE-2014-6271 Bash/Shellshock

Overview:

Source: US-CERT/NIST

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." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.

External sources:

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271>

Vulnerable products, firmware and applications:

No Axis products are affected as BASH (Bourne Again Shell) is not included in the firmware.

Impact on Axis products, systems and users:

None.

Axis recommendations:

N/A

Axis plan:

N/A