

CVE-2014-6278

GNU Bash OS Command Injection Vulnerability

CISA KEV since Oct 2, 2025

Actively exploited

Public exploit module (Metasploit)

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.

EVRS 87 / 100 Immediate priority	CVSS V3.1 8.8 High · NVD	EPSS 0.996 99.95th percentile · FIRST	CISA DEADLINE Oct 23, 2025 KEV since 2025 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.996 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability could affect an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products.

Basis: CISA KEV required action

NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
bash	1.14.0	no fixed version listed	NVD
	1.14.1		
	1.14.2		
	1.14.3		
	1.14.4		
	1.14.5		
	1.14.6		
	1.14.7		
	2.0		
	2.01		
	2.01.1		
	2.02		
	2.02.1		
	2.03		
	2.04		
	2.05		
	3.0		
	3.0.16		
	3.1		
	3.2		
	3.2.48		
	4.0		
	4.1		
	4.2		
	4.3		

Sources

Vendor guidance	github.com/advisories/GHSA-6493-28fj-f93w	Additional guidance	suse.com/support/shellshock/
ftp.gnu.org	ftp.gnu.org/gnu/bash/bash-4.3-patches/bash43-027	support.broadcom.com	support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23467
sec.cloudapps.cisco.com	sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140926-bash	ibm.com	ibm.com/support/pages/security-bulletin-update-vulnerabilities-bash-affect-aix-toolbox-linux-applications-cve-2014-6271-cve-2014-6277-cve-2014-6278-cve-2014-7169-cve-2014-7186-and-cve-2014-7187
NVD	nvd.nist.gov/vuln/detail/CVE-2014-6278	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2014-6163	Current data	evulnable.com/vulnerability-management/cve/CVE-2014-6278

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.