

CVE-2015-3246

Red Hat Libuser Race Condition Vulnerability

CISA KEV since Aug 26, 2026

Actively exploited

Public exploit module (Metasploit)

libuser before 0.56.13-8 and 0.60 before 0.60-7, as used in the userhelper program in the usermode package, directly modifies /etc/passwd, which allows local users to cause a denial of service (inconsistent file state) by causing an error during the modification. NOTE: this issue can be combined with CVE-2015-3245 to gain privileges.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.4 High · NVD	EPSS 0.085 95th percentile · FIRST	CISA DEADLINE Sep 9, 2026 CISA federal deadline · Overdue by 43 days
---	--	--	--

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 90 days
☒ EPSS	0.085 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines. **CISA note:** This vulnerability affects an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
libuser	< 0.56.13-8 ≥ 0.60 < 0.60-7	no fixed version listed	NVD
enterprise linux	5.0 6.0 7.0	no fixed version listed	NVD
opensuse	13.2	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-f52h-j689-x786	access.redhat.com	access.redhat.com/articles/1537873
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2015-3246	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2015-3301	Current data	evulnable.com/vulnerability-management/cve/CVE-2015-3246

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