CVE-2025-61662

VEX

Public on November 18, 2025
Last modified: March 16, 2026 at 7:20:09 PM UTC

MODERATE

Moderate severity
What does this mean?

7.8

CVSS v3 Score Breakdown

Jump to section

Description Statement Mitigation Additional information Affected Packages CVSS Score Details FAQ

Description

A Use-After-Free vulnerability has been discovered in GRUB's gettext module. This flaw stems from a programming error where the gettext command remains registered in memory after its module is unloaded. An attacker can exploit this condition by invoking the orphaned command, causing the application to access a memory location that is no longer valid. An attacker could exploit this vulnerability to cause grub to crash, leading to a Denial of Service. Possible data integrity or confidentiality compromise is not discarded.

Statement

This vulnerability has been rated as have the impact of Moderate by the Red Hat Product Security team. This decision was made based in the fact an attacker needs local or physic al access to the machine, to execute the gettext command after it was unloaded. Additio nally the most likely outcome from an successful attack is a Denial of Crash by leading th e grub2 to crash.

Mitigation

There's no known mitigation available for this vulnerability.

Additional information

- Bugzilla 2414683: grub2: Missing unregister call for gettext command may lead to use-after-free

External references

- https://www.cve.org/CVERecord?id=CVE-2025-61662
- https://nvd.nist.gov/vuln/detail/CVE-2025-61662
- https://lists.gnu.org/archive/html/grub-devel/2025-11/msg00155.html

Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat Enterprise Linux 10
Components	grub2
State	Fixed
Justification	None
Errata	RHSA-2026:4649
Release Date	March 16, 2026

Products / Services	Red Hat Enterprise Linux 10.0 Extended Update Support
Components	grub2
State	Fixed
Justification	None
Errata	RHSA-2026:4652
Release Date	March 16, 2026

Products / Services	Red Hat Enterprise Linux 7 Extended Lifecycle Support
Components	grub2
State	Fixed
Justification	None
Errata	RHSA-2026:5233

1 of 2

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	7.8	7.8	N/A
Attack Vector	Local	Local	N/A
Attack Complexity	Low	Low	N/A
Privileges Required	Low	Low	N/A
User Interaction	None	None	N/A
Scope	Unchanged	Unchanged	N/A
Confidentiality Impact	High	High	N/A
Integrity Impact	High	High	N/A
Availability Impact	High	High	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Frequently Asked Questions

Why is Red Hat's CVSS v3 score or Impact different from other vendors?

My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?

What can I do if my product is listed as "Will not fix"?

What can I do if my product is listed as "Fix deferred"?

What is a mitigation?

I have a Red Hat product but it is not in the above list, is it affected?

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: March 16, 2026 at 7:20:09 PM UTC

Red Hat

Quick Links

Help

Site Info

Related Sites

⚠ Partial system outage

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility