Grub2: missing unregister call for gettext command may lead to use-after-free

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-61662
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-11-18 19:15:50 UTC
Updated	2026-04-16 14:16:12 UTC
Description	A Use-After-Free vulnerability has been discovered in GRUB's gettext module. This flaw stems from a programming error w

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

EPSS: 0.000120000 probability, percentile 0.016600000 (date 2026-04-19)

Problem Types: CWE-416 | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	secalert@redhat.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

vailability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Grub2	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	GNU	Grub2	affected 2.14 semver
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 1:2.12-29.el10_1.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 10.0 Extended Update Support	unaffected 1:2.12-15.el10_0.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 1:2.02-0.87.el7_9.16 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 1:2.02-170.el8_10.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 1:2.02-87.el8_2.14 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 1:2.02-99.el8_4.13 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 1:2.02-99.el8_4.13 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 1:2.02-123.el8_6.19 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 1:2.02-123.el8_6.19 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 1:2.02-123.el8_6.19 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 1:2.02-152.el8_8.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 1:2.02-152.el8_8.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 1:2.06-114.el9_7.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 1:2.06-27.el9_0.23 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 1:2.06-61.el9_2.11 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 1:2.06-86.el9_4.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.6 Extended Update Support	unaffected 1:2.06-105.el9_6.1 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.12	unaffected 412.86.202604010116-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.13	unaffected 413.92.202604080111-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.18	unaffected 418.94.202603181125-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.19	unaffected 4.19.9.6.202604080618-0 * rpm

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:4654	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4649	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4823	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5074	secalert@redhat.com	access.redhat.com	
lists.gnu.org/archive/html/grub-devel/2025-11/msg00155.html	secalert@redhat.com	lists.gnu.org	
access.redhat.com/errata/RHSA-2026:4998	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5233	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5127	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4830	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2025-61662	secalert@redhat.com	access.redhat.com	Third Party
access.redhat.com/errata/RHSA-2026:7243	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4652	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4900	secalert@redhat.com	access.redhat.com	
www.openwall.com/lists/oss-security/2025/11/18/5	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing Lis
access.redhat.com/errata/RHSA-2026:6492	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4648	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4822	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Trac
access.redhat.com/errata/RHSA-2026:4653	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7239	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4760	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-11-12T21:18:21.069Z	Reported to Red Hat.
CNA	2025-11-18T00:00:00.000Z	Made public.

Workarounds

CNA: There's no known mitigation available for this vulnerability.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**