Gnuplot: segmentation fault via io_str_init_static_internal function

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

Summary

CVE	CVE-2025-3359
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-07 13:15:43 UTC
Updated	2026-05-03 10:16:15 UTC
Description	A flaw was found in GNUPlot. A segmentation fault via IO_str_init_static_internal may jeopardize the environment.

Risk And Classification

Primary CVSS: v3.1 6.2 MEDIUM from secalert@redhat.com

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

Problem Types: CWE-754 | CWE-754 Improper Check for Unusual or Exceptional Conditions

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6.2	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.2	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2025-3359	secalert@redhat.com	access.redhat.com	
sourceforge.net/p/gnuplot/bugs/2781	secalert@redhat.com	sourceforge.net	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank ChenYiFan Liu for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-04-07T01:36:42.665Z	Reported to Red Hat.
CNA	2025-04-07T00:00:00.000Z	Made public.

Workarounds

CNA: Currently, no mitigation is available for this vulnerability.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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