



# Gnuplot: segmentation fault via io\_str\_init\_static\_internal function

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2025-3359
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-04-07 13:15:43 UTC
<b>Updated</b>	2026-05-03 10:16:15 UTC
<b>Description</b>	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	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 6</a>	Not specified	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 7</a>	Not specified	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 8</a>	Not specified	Not specified

### References

Reference	Source	Link	Tags
<a href="https://access.redhat.com/security/cve/CVE-2025-3359">access.redhat.com/security/cve/CVE-2025-3359</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://sourceforge.net/p/gnuplot/bugs/2781">sourceforge.net/p/gnuplot/bugs/2781</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://sourceforge.net">sourceforge.net</a>	
<a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This

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

CVE, CWE, and OVAL are registered 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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)