



## Bug 2357749 (CVE-2025-3359) - CVE-2025-3359 gnuplot: Segmentation fault via IO\_str\_init\_static\_internal function

**Keywords:** Security

**Reported:** 2025-04-07 01:40 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2025-09-13 23:00 UTC ([History](#))

**Alias:** CVE-2025-3359

**CC List:** 1 user ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:** [2357751](#) [2357752](#)

**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)

**Attachments** ([Terms of Use](#))

OSIDB Bzimport 2025-04-07 01:40:13 UTC

[Description](#)

A flaw was found in GNUPlot. A segmentation fault via IO\_str\_init\_static\_internal may jeopardize the environment.

Orion Poplawski 2025-09-13 23:00:59 UTC

[Comment 2](#)

This is fixed upstream with this commit:

```
commit a5897feadc4be73b0ffd8458556c47117bd24d03
Author: Ethan A Merritt <merritt.edu>
```

Date: Tue Mar 25 22:51:54 2025 -0700

```
hpgl: font name parsing overruns the string by one char
```

```
if no comma is present in the font name.
```

```
E.g.
```

```
set term pcl
```

```
set title "Title" font "sans" # no comma in font
```

```
name
```

```
plot x
```

[Bug-2781](#)

Not yet released.

---

Note

You need to [log in](#) before you can comment on or make changes to this bug.

