CVE-2025-31177

Public on March 27, 2025
Last Modified: May 7, 2025 at 8:55:01 PM UTC

MODERATE

Moderate Impact
What does this mean?

6.2

CVSS v3 Score Breakdown

Jump to section

escription | Statement | Mitigation | Additional information | Affected Packages | CVSS Score Details | Weakness (CWE) | Acknowledgements | FA

Description

gnuplot is affected by a heap buffer overflow at function utf8_copy_one.

Statement

This flaw is rated as a Moderate impact as the attacker or malicious user must be local and the impact is restricted to availability.

Mitigation

Currently, no mitigation is available for this vulnerability

Additional information

- Bugzilla 2355342: gnuplot: gnuplot heap-buffer overflow on utf8_copy_one
- CWE-122: Heap-based Buffer Overflow

External references

- https://www.cve.org/CVERecord?id=CVE-2025-31177
- https://nvd.nist.gov/vuln/detail/CVE-2025-31177

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State | Errata | Clear all

Products / Services	Components	State	Errata	Release Date
Red Hat Enterprise Linux 6	gnuplot	Out of support scope		
Red Hat Enterprise Linux 7	gnuplot	Out of support scope		
Red Hat Enterprise Linux 8	gnuplot	Out of support scope		

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.

1-10 of 3

1 of 1

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).

The following CVSS metrics and score provided are preliminary and subject to review.

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	6.2	N/A
Attack Vector	Local	N/A
Attack Complexity	Low	N/A
Privileges Required	None	N/A
User Interaction	None	N/A
Scope	Unchanged	N/A
Confidentiality Impact	None	N/A
Integrity Impact	None	N/A
Availability Impact	High	N/A

CVSS v3 Vector

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

Understanding the Weakness (CWE)

CWE-122

Availability

Technical Impact: DoS: Crash, Exit, or Restart; DoS: Resource Consumption (CPU); DoS: Resource Consumption (Memory)

Buffer overflows generally lead to crashes. Other attacks leading to lack of availability are possible, including putting the program into an infinite loop.

Integrity,Confidentiality,Availability,Access Control

Technical Impact: Execute Unauthorized Code or Commands; Bypass Protection Mechanism; Modify Memory

Buffer overflows often can be used to execute arbitrary code, which is usually outside the scope of a program's implicit security policy. Besides important user data, heap-based overflows can be used to overwrite function pointers that may be living in memory, pointing it to the attacker's code. Even in applications that do not explicitly use function pointers, the run-time will usually leave many in memory. For example, object methods in C++ are generally implemented using function pointers. Even in C programs, there is often a global offset table used by the underlying runtime.

Integrity,Confidentiality,Availability,Access Control,Other

Technical Impact: Execute Unauthorized Code or Commands; Bypass Protection Mechanism; Other

When the consequence is arbitrary code execution, this can often be used to subvert any other security service.

Acknowledgements

Red Hat would like to thank ChenYiFan Liu for reporting this issue.

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?

My product is listed as "Out of Support Scope". What does this mean?

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: May 7, 2025 at 8:55:01 PM UTC