



# systemd: Local unprivileged user can trigger an assert

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-29111  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | GitHub_M  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-03-23 22:16:26 UTC   |
| <b>Updated</b>         | 2026-04-15 16:44:38 UTC   |
| <b>Description</b>     | systemd, a system and service manager, (as PID 1) hits an assert and freezes execution when an unprivileged IPC API cal |

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from security-advisories@github.com

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

**Problem Types:** CWE-269 | NVD-CWE-noinfo | CWE-269 CWE-269: Improper Privilege Management

| Version | Source                         | Type      | Score | Severity | Vector  |
|---------|--------------------------------|-----------|-------|----------|---|
| 3.1     | security-advisories@github.com | Secondary | 5.5   | MEDIUM   | <b>CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</b> |
| 3.1     | CNA                            | DECLARED  | 5.5   | MEDIUM   | <b>CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</b> |

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor          | Product | Version | Update | Edition | Language |
|-------------|-----------------|---------|---------|--------|---------|----------|
| Application | Systemd Project | Systemd | All     | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor  | Product | Version                   | Platforms     |
|--------|---------|---------|---------------------------|---------------|
| CNA    | Systemd | Systemd | affected >= 239, < 257.11 | Not specified |
| CNA    | Systemd | Systemd | affected >= 258, < 258.5  | Not specified |
| CNA    | Systemd | Systemd | affected >= 259, < 259.2  | Not specified |

References

| Reference  | Source                         | Link         | T |
|--|--------------------------------|--------------|---|
| github.com/systemd/systemd/commit/7ac3220213690e8a8d6d2a6e81e43bd1dce01d69 | security-advisories@github.com | github.com   | F |
| github.com/systemd/systemd/commit/42aee39107fbdd7db1ccd402a2151822b2805e9f | security-advisories@github.com | github.com   | F |
| github.com/systemd/systemd/commit/54588d2dedff54bf6036670820650e4ea74628f  | security-advisories@github.com | github.com   | F |
| github.com/systemd/systemd/commit/20021e7686426052e3a7505425d7e12085feb2a6 | security-advisories@github.com | github.com   | F |
| github.com/systemd/systemd/commit/1d22f706bd04f45f8422e17fbde3f56ece17758a | security-advisories@github.com | github.com   | F |
| github.com/systemd/systemd/commit/21167006574d6b83813c7596759b474f56562412 | security-advisories@github.com | github.com   | F |
| github.com/systemd/systemd/commit/efa6ba2ab625aaa160ac435a09e6482fc63bdbe8 | security-advisories@github.com | github.com   | F |
| github.com/systemd/systemd/commit/b5fd14693057e5f2c9b4a49603be64ec3608ff6c | security-advisories@github.com | github.com   | F |
| github.com/systemd/systemd/security/advisories/GHSA-gx6q-6f99-m764         | security-advisories@github.com | github.com   | F |
| github.com/systemd/systemd/commit/3cee294fe8cf4fa0eff933ab21416d099942cabd | security-advisories@github.com | github.com   | F |
| github.com/systemd/systemd/commit/80acea4ef80a4bb78560ed970c34952299b890d6 | security-advisories@github.com | github.com   | F |
| CVE Program record   | CVE.ORG                        | www.cve.org  | c |
| NVD vulnerability detail   | NVD                            | nvd.nist.gov | c |

No vendor comments have been submitted for this CVE.

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

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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)