



# CVE-2023-25267

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2023-25267  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2023-03-15 22:15:00 UTC   |
| <b>Updated</b>         | 2023-03-24 16:25:00 UTC   |
| <b>Description</b>     | An issue was discovered in GFI Kerio Connect 9.4.1 patch 1 (fixed in 10.0.0). There is a stack-based Buffer Overflow in the |

## Risk And Classification

**Problem Types: CWE-787**

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product       | Version | Update | Edition | Language |
|-------------|--------|---------------|---------|--------|---------|----------|
| Application | Gfi    | Kerio Connect | 9.4.1   | patch1 | All     | All      |

## References

| Reference                   | Source  | Link  | Tags                |
|-----------------------------|---------|---|---------------------|
| kerioconnectPoC.md · GitHub | MISC    | <a href="https://gist.github.com">gist.github.com</a>                           |                     |
| Security check              | MISC    | <a href="https://support.kerioconnect.gfi.com">support.kerioconnect.gfi.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 |

No vendor comments have been submitted for this CVE.

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

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)