



CVE-2022-43612

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2022-43612 |
| State | PUBLIC |
| Assigner | zdi-disclosures@trendmicro.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-03-29 19:15:00 UTC |
| Updated | 2023-04-10 14:10:00 UTC |
| Description | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Corel CorelDRAW Gr |

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|-----------|------------|--------|---------|----------|
| Application | Corel | Coreldraw | All | All | All | All |
| Application | Corel | Coreldraw | 23.5.0.506 | All | All | All |

References

| Reference | Source | Link | Tags |
|-----------------------------------|---------|--|---------------------|
| ZDI-22-1470 Zero Day Initiative | MISC | www.zerodayinitiative.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | 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

CVE.report and Source URL Uptime Status status.cve.report