



# CVE-2022-28368

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

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2022-28368                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                       |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2022-04-03 03:15:00 UTC                                                                                                      |
| <b>Updated</b>         | 2023-08-08 14:22:00 UTC                                                                                                      |
| <b>Description</b>     | Dompdf 1.2.1 allows remote code execution via a .php file in the src:url field of an @font-face Cascading Style Sheets (CSS) |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                         | Product                | Version | Update | Edition | Language |
|-------------|--------------------------------|------------------------|---------|--------|---------|----------|
| Application | <a href="#">Dompdf Project</a> | <a href="#">Dompdf</a> | All     | All    | All     | All      |

## References

| Reference                                                                                                 | Source  | Link                                    |
|-----------------------------------------------------------------------------------------------------------|---------|-----------------------------------------|
| Match installed font filename extension to type by bsweeney · Pull Request #2808 · dompdf/dompdf · GitHub | MISC    | <a href="#">github.com</a>              |
| Dompdf 1.2.1 Remote Code Execution ~ Packet Storm                                                         | MISC    | <a href="#">packetstormsecurity.com</a> |
| dompdf security alert: RCE vulnerability found in popular PHP PDF library   Snyk                          | MISC    | <a href="#">snyk.io</a>                 |
| dompdf/dompdf - Packagist                                                                                 | MISC    | <a href="#">packagist.org</a>           |
| GitHub - snyk-labs/php-goof: Snyk PHP Goof - A vulnerable PHP demo application                            | MISC    | <a href="#">github.com</a>              |
| Match installed font filename extension to type · dompdf/dompdf@4c70e10 · GitHub                          | MISC    | <a href="#">github.com</a>              |
| Remote code execution vulnerability through persisted font · Issue #2598 · dompdf/dompdf · GitHub         | MISC    | <a href="#">github.com</a>              |
| CVE Program record                                                                                        | CVE.ORG | <a href="#">www.cve.org</a>             |
| NVD vulnerability detail                                                                                  | NVD     | <a href="#">nvd.nist.gov</a>            |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)