



ImageMagick Engine <= 1.7.5 - Cross-Site Request Forgery to Remote Command Execution

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2022-2441 |
| State | PUBLISHED |
| Assigner | Wordfence |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-10-20 08:15:11 UTC |
| Updated | 2026-04-08 19:17:51 UTC |
| Description | The ImageMagick Engine plugin for WordPress is vulnerable to remote code execution via the 'cli_path' parameter in versio |

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

EPSS: 0.018980000 probability, percentile 0.832190000 (date 2026-04-09)

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | security@wordfence.com | Secondary | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | CNA | DECLARED | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-----------|--------------------|---------|--------|---------|----------|
| Application | Orangelab | Imagemagick Engine | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|----------|--------------------|-----------------------|---------------|
| CNA | Rickardw | ImageMagick Engine | affected 1.7.5 semver | Not specified |

References

| Reference | Source |
|---|--------------------|
| imagemagick-engine/imagemagick-engine.php at v.1.7.2 · orangelabweb/imagemagick-engine · GitHub | af854a3a-2127-4221 |
| Vulnerability Advisories Continued - Wordfence | af854a3a-2127-4221 |
| imagemagick-engine/imagemagick-engine.php at 1.7.4 · orangelabweb/imagemagick-engine · GitHub | af854a3a-2127-4221 |
| 403 Forbidden | af854a3a-2127-4221 |
| Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated) - PHP webapps Exploit | af854a3a-2127-4221 |
| ImageMagick Engine <= 1.7.5 - Cross-Site Request Forgery to Remote Command Execution | af854a3a-2127-4221 |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

Vendor Comments And Credit

Discovery Credit

CNA: Rasoul Jahanshahi (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|-----------|
| CNA | 2022-10-17T00:00:00.000Z | Disclosed |

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](#)