



WP Force SSL & HTTPS SSL Redirect <= 1.66 - Missing Authorization to Settings Update

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2024-5770 |
| State | PUBLISHED |
| Assigner | Wordfence |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2024-06-08 05:15:40 UTC |
| Updated | 2026-04-08 19:22:00 UTC |
| Description | The WP Force SSL & HTTPS SSL Redirect plugin for WordPress is vulnerable to unauthorized modification of data due to |

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from nvd@nist.gov

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

EPSS: 0.000720000 probability, percentile 0.221360000 (date 2026-04-10)

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 4.3 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N |
| 3.1 | security@wordfence.com | Secondary | 4.2 | MEDIUM | CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L |
| 3.1 | CNA | DECLARED | 4.2 | MEDIUM | CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------------|--------------|---------|--------|---------|----------|
| Application | WebfactoryLtd | Wp Force Ssl | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|------------|---------------------------------|----------------------|---------------|
| CNA | Webfactory | WP Force SSL HTTPS SSL Redirect | affected 1.66 semver | Not specified |

References

| Reference | Source | Link |
|--|--------------------------------------|-----------|
| plugins.trac.wordpress.org/changeset/3099110 | af854a3a-2127-422b-91ae-364da2661108 | plugins.t |
| plugins.trac.wordpress.org/browser/wp-force-ssl/tags/1.66/wp-force-ssl.php | af854a3a-2127-422b-91ae-364da2661108 | plugins.t |
| www.wordfence.com/threat-intel/vulnerabilities/id/c2081e4a-c6b7-4730-be59-bc728... | af854a3a-2127-422b-91ae-364da2661108 | www.wo |
| swisskyrepo.github.io/PayloadsAllTheThings/CRLF%20Injection | af854a3a-2127-422b-91ae-364da2661108 | swisskyr |
| CVE Program record | CVE.ORG | www.cve |
| NVD vulnerability detail | NVD | nvd.nist. |

Vendor Comments And Credit

Discovery Credit

CNA: Friderika Baranyai (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|-----------|
| CNA | 2024-06-07T00:00:00.000Z | Disclosed |

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

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