



WordPress FileBird plugin <= 5.1.4 - Broken Access Control vulnerability

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-25966 |
| State | PUBLISHED |
| Assigner | Patchstack |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2024-12-09 13:15:24 UTC |
| Updated | 2026-04-28 19:19:52 UTC |
| Description | Missing Authorization vulnerability in Ninja Team Filebird allows Exploiting Incorrectly Configured Access Control Security L |

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.002960000 probability, percentile 0.528710000 (date 2026-05-12)

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

| Version | Source | Type | Score | Severity | Vector |
|---------|----------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 6.5 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N |
| 3.1 | audit@patchstack.com | Secondary | 5.5 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N |
| 3.1 | CNA | CVSS | 5.5 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-----------|----------|---------|--------|---------|----------|
| Application | Ninjateam | Filebird | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|------------|----------|---------------------------|---------------|
| CNA | Ninja Team | Filebird | affected n/a 5.1.4 custom | Not specified |

References

Reference

patchstack.com/database/wordpress/plugin/filebird/vulnerability/wordpress-fi...

https://patchstack.com/database/wordpress/plugin/filebird/vulnerability/wordpress-filebird-plugin-5-1-4-broken-access-control-vulnerability?_s...

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: Rafshanzani Suhada (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress Filebird plugin to the latest available version (at least 5.1.5).

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