



Active Directory Integration / LDAP Integration <= 4.1.4 - Cross-Site Request Forgery to SQL Injection

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

Summary

CVE	CVE-2023-2599
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-09 06:16:10 UTC
Updated	2026-04-08 18:18:04 UTC
Description	The Active Directory Integration plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to time-based SC

Risk And Classification

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

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

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	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	security@wordfence.com	Secondary	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L
3.1	CNA	DECLARED	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miniorange	Active Directory Integration / Ldap Integration	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cyberlord92	Active Directory Integration / LDAP Integration	affected 4.1.4 semver	Not specified

References

Reference	Source
403 Forbidden	af854a3a-2127-422b-91ae-364da26f
Active Directory Integration / LDAP Integration <= 4.1.4 - Cross-Site Request Forgery to SQL Injection	af854a3a-2127-422b-91ae-364da26f
403 Forbidden	af854a3a-2127-422b-91ae-364da26f
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Marco Wotschka (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-05-02T00:00:00.000Z	Discovered
CNA	2023-05-12T00:00:00.000Z	Disclosed

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

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