



Staff / Employee Business Directory for Active Directory <= 1.2.3 - Authenticated (Admin+) LDAP Passback

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

Summary

CVE	CVE-2023-4505
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-27 15:19:40 UTC
Updated	2026-04-08 17:17:02 UTC
Description	The Staff / Employee Business Directory for Active Directory plugin for WordPress is vulnerable to LDAP Passback in versi

Risk And Classification

Primary CVSS: v3.1 4.9 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-306 | CWE-306 CWE-306 Missing Authentication for Critical Function

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
3.1	security@wordfence.com	Secondary	2.2	LOW	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	2.2	LOW	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miniorange	Staff / Employee Business Directory For Active Directory	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cyberlord92	Staff/Employee Business Directory For Active Directory	affected 1.2.3 semver	Not specified

References

Reference	Source
plugins.trac.wordpress.org/changeset/2973020	security@wordfence.com
Staff / Employee Business Directory for Active Directory <= 1.2.3 - Authenticated (Admin+) LDAP Passback	af854a3a-2127-422b-91ae-364
Staff / Employee Business Directory for Active Directory – WordPress plugin WordPress.org	af854a3a-2127-422b-91ae-364
CVE-2023–4506 & CVE-2023–4505: LDAP Passback on miniOrange Medium	af854a3a-2127-422b-91ae-364
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Pedro José Navas Pérez (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-09-25T00:00:00.000Z	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