



Improper permission checks in Extension:NSFileRepo

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

Summary

CVE	CVE-2026-24732
State	PUBLISHED
Assigner	HW
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-04 13:15:58 UTC
Updated	2026-04-28 21:06:10 UTC
Description	Files or Directories Accessible to External Parties, Incorrect Permission Assignment for Critical Resource vulnerability in Ha

Risk And Classification

Primary CVSS: v4.0 6.6 MEDIUM from security@bluespice.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:P/AU:Y/R:X/V:X/RE:L/U:X

EPSS: 0.000590000 probability, percentile 0.181700000 (date 2026-04-28)

Problem Types: CWE-552 | CWE-732 | CWE-552 CWE-552 Files or Directories Accessible to External Parties | CWE-732 CWE-732 Incorrect Permission Assignment for Critical Resource

Version	Source	Type	Score	Severity	Vector
4.0	security@bluespice.com	Secondary	6.6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
4.0	CNA	CVSS	6.6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:P/AU:Y/R:X/V:X/RE:L/U:X

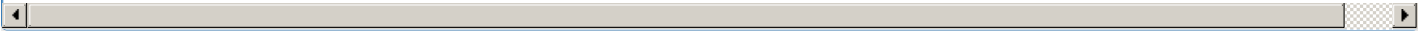


Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Hallo Welt! GmbH	BlueSpice	affected 5.1 5.1.3 semver	Not specified
CNA	Hallo Welt! GmbH	BlueSpice	affected 5.2 5.2.0 semver	Not specified

References

Reference	Source	Link	Tags
en.wiki.bluespice.com/wiki/Security:Security_Advisories/BSSA-2026-02	security@bluespice.com	en.wiki.bluespice.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy



No vendor comments have been submitted for this CVE.

Additional Advisory Data

Workarounds

CNA: Make sure \$wgGroupPermissions['*']['read'] is set to false in the LocalSettings.php.

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