WordPress Asgaros Forum plugin <= 3.0.0 - File Upload Numbers Bypass vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-32227
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-10 08:15:19 UTC
Updated	2026-04-29 10:16:45 UTC
Description	Authentication Bypass by Spoofing vulnerability in Asgaros Asgaros Forum asgaros-forum allows Identity Spoofing.This iss

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.001280000 probability, percentile 0.317300000 (date 2026-05-03)

Problem Types: CWE-290 | CWE-290 Authentication Bypass by Spoofing

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Asgaros	Asgaros Forum	affected 3.0.0 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/asgaros-forum/vulnerability/wordpre...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

Vendor Comments And Credit

Discovery Credit

CNA: 20kilograma | Patchstack Bug Bounty Program (en)

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