WeGIA has SQL Injection via Session Variable Override in DespachoControle.php

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

Summary

CVE	CVE-2026-40285
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 21:16:34 UTC
Updated	2026-04-20 19:02:18 UTC
Description	WeGIA is a web manager for charitable institutions. Versions prior to 3.6.10 contain a SQL injection vulnerability in dao/mer

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from security-advisories@github.com

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

EPSS: 0.000350000 probability, percentile 0.102190000 (date 2026-04-21)

Problem Types: CWE-89 | CWE-302 | CWE-473 | CWE-89 CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | CWE-302 CWE-302: Authentication Bypass by Assumed-Immutable Data | CWE-473 CWE-473: PHP External Variable Modification

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	LabRedesCefetRJ	WeGIA	affected < 3.6.10	Not specified

References

Reference	Source	Link
github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-666r-v2m7-xgp9	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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 registred 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**