CVE-2026-31843

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

Summary

CVE	CVE-2026-31843
State	PUBLISHED
Assigner	TuranSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-16 13:16:48 UTC
Updated	2026-04-17 15:38:09 UTC
Description	The goodoneuz/pay-uz Laravel package (<= 2.2.24) contains a critical vulnerability in the /payment/api/editable/update end

Risk And Classification

Primary CVSS: v4.0 10 CRITICAL from 309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c

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

EPSS: 0.008860000 probability, percentile 0.754750000 (date 2026-04-21)

Problem Types: CWE-284 | CWE-284 CWE-284 Improper Access Control leading to unauthorized modification of executable application files

Version	Source	Type	Score	Severity	Vector
4.0	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA
4.0	CNA	CVSS	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA
3.1	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C
2.0	CNA	CVSS	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Goodoneuz	Pay-uz	affected <= 2.2.24	Not specified

References

Reference	Source	Link	Ta
github.com/shaxzodbek-uzb/pay-uz	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	github.com	
github.com/goodoneuz/pay-uz/blob/master/src/Http/Controllers/ApiControll...	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	github.com	
github.com/goodoneuz/pay-uz/blob/master/src/routes/web.php	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	github.com	
packagist.org/packages/goodoneuz/pay-uz	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	packagist.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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