

CVE-2021-32648

October CMS Improper Authentication

Exigent

CISA KEV since Jan 18, 2022

Actively exploited

octobercms is a CMS platform based on the Laravel PHP Framework. In affected versions of the october/system package an attacker can request an account password reset and then gain access to the account using a specially crafted request. The issue has been patched in Build 472 and v1.1.5.

EVRS 85/100 Immediate priority	CVSS V3.1 9.1 Critical · NVD	EPSS 0.904 99.8th percentile · FIRST	CISA DEADLINE Feb 1, 2022 KEV since 2022 · listed over a year
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.904 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
october	≥ 1.1.1 < 1.1.5 1.0.471	1.1.5	NVD

Sources

Vendor guidance github.com/octobercms/library/commit/016a297b1bec55d2e53bc889458ed2cb5c3e9374
NVD nvd.nist.gov/vuln/detail/CVE-2021-32648

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-1808

Additional guidance github.com/octobercms/october/security/advisories/GHSA-mxr5-mc97-63rc
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnabile.com/vulnerability-management/cve/CVE-2021-32648

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.