

CVE-2018-15133

Laravel Deserialization of Untrusted Data Vulnerability

CISA KEV since Jan 16, 2024

Actively exploited

Public exploit module (Metasploit)

In Laravel Framework through 5.5.40 and 5.6.x through 5.6.29, remote code execution might occur as a result of an unserialize call on a potentially untrusted X-XSRF-TOKEN value. This involves the decrypt method in Illuminate/Encryption/Encrypter.php and PendingBroadcast in gadgetchains/Laravel/RCE/3/chain.php in phpggc. The attacker must know the application key, which normally would never occur, but could happen if the attacker previously had privileged access or successfully accomplished a previous attack.

EVRS 79/₁₀₀ Urgent priority	CVSS V3.1 8.1 High · NVD	EPSS 0.766 99.54th percentile · FIRST	CISA DEADLINE Feb 6, 2024 KEV since 2024 · 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	0.766 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
laravel/framework	≤ 5.5.40	no fixed version listed	GitHub
laravel/framework	≥ 5.6.0, ≤ 5.6.29	5.6.30	GitHub
laravel	≤ 5.5.40 ≥ 5.6.0 ≤ 5.6.29	after 5.5.40 · after 5.6.29	NVD

Sources

Vendor guidance github.com/advisories/GHSA-qvqm-h22r-4cp9
NVD nvd.nist.gov/vuln/detail/CVE-2018-15133

Additional guidance laravel.com/docs/5.6/upgrade#upgrade-5.6.30
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-5039

Current data evulnable.com/vulnerability-management/cve/CVE-2018-15133

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