

CVE-2019-9978

WordPress Social Warfare Plugin Cross-Site Scripting (XSS) Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

The social-warfare plugin before 3.5.3 for WordPress has stored XSS via the wp-admin/admin-post.php?swp_debug=load_options swp_url parameter, as exploited in the wild in March 2019. This affects Social Warfare and Social Warfare Pro.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 6.1 Medium · NVD	EPSS 0.729 99.45th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	0.729 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
social warfare	< 3.5.3	3.5.3	NVD
social warfare pro	< 3.5.3	3.5.3	NVD

Sources

Vendor guidance	blog.sucuri.net/2019/03/zero-day-stored-xss-in-social-warfare.html	Additional guidance	twitter.com/warfareplugins/status/1108852747099652099
Additional guidance	wpvulndb.com/vulnerabilities/9238	NVD	nvd.nist.gov/vuln/detail/CVE-2019-9978
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-19332
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-9978		

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