



# SocialEngine <= 7.8.0 Blind SSRF via /core/link/preview

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-41461
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-23 15:37:24 UTC
<b>Updated</b>	2026-04-23 18:16:29 UTC
<b>Description</b>	SocialEngine versions 7.8.0 and prior contain a blind server-side request forgery vulnerability in the /core/link/preview endpoint

## Risk And Classification

**Primary CVSS:** v4.0 6.3 MEDIUM from disclosure@vulncheck.com

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

**Problem Types:** CWE-918 | CWE-918 CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/SA:N
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/SA:N
3.1	disclosure@vulncheck.com	Primary	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N
3.1	CNA	CVSS	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality: None  
 Integrity: Low  
 Availability: None  
 Sub Conf.: High  
 Sub Integrity: Low  
 Sub Availability: None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C: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: Low  
 User Interaction: None  
 Scope: Changed  
 Confidentiality: High  
 Integrity: Low  
 Availability: None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SocialEngine	SocialEngine	affected 7.8.0 semver	Not specified

### References

Reference	Source	Link	Tags
karmainsecuritv.com/KIS-2026-07	disclosure@vulncheck.com	karmainsecuritv.com	

www.vulncheck.com/advisories/socialengine-blind-ssrf-via-core-link-preview	disclosure@vulncheck.com	www.vulncheck.com	
socialengine.com	disclosure@vulncheck.com	socialengine.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

## Vendor Comments And Credit

### Discovery Credit

**CNA: Egidio Romano (en)**

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 registered 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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)