



# Beghelli Sicuro24 SicuroWeb Missing Content Security Policy

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

## Summary

<b>CVE</b>	CVE-2026-41469
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-22 19:17:09 UTC
<b>Updated</b>	2026-04-22 21:18:45 UTC
<b>Description</b>	Beghelli Sicuro24 SicuroWeb does not enforce a Content Security Policy, allowing unrestricted loading of external JavaScript

## Risk And Classification

**Primary CVSS:** v4.0 5.1 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-693 | CWE-693 CWE-693 Protection Mechanism Failure

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N
3.1	disclosure@vulncheck.com	Primary	5.2	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	5.2	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Passive

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Beghelli	SicuroWeb Sicuro24	affected	Not specified

### References

Reference	Source	Link
aithub.com/kmkz/Exploits/blob/master/2026/CVE-2026-22191-POC.pv	disclosure@vulncheck.com	<a href="https://aithub.com">aithub.com</a>

github.com/kmkz/Exploits/blob/master/2026/CVE-2026-22191-SicuroWeb-ATI-c...	disclosure@vulncheck.com	github.com
www.boffsec-services.com/posts/sicuroweb-cve-2026-22191	disclosure@vulncheck.com	www.boffsec-services.c
www.beghelli.it	disclosure@vulncheck.com	www.beghelli.it
www.vulncheck.com/advisories/beghelli-sicuro24-sicuroweb-missing-content-securi...	disclosure@vulncheck.com	www.vulncheck.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Jean-Marie Bourbon of Bourbon Offensive Security Services (en)

**CNA:** VulnCheck (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)