



# Beghelli Sicuro24 SicuroWeb AngularJS Sandbox Escape via Template Injection

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

## Summary

<b>CVE</b>	CVE-2026-41468
<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 19:17:08 UTC
<b>Updated</b>	2026-04-22 21:18:45 UTC
<b>Description</b>	Beghelli Sicuro24 SicuroWeb embeds AngularJS 1.5.2, an end-of-life component containing known sandbox escape primiti

## Risk And Classification

**Primary CVSS:** v4.0 9.3 CRITICAL from disclosure@vulncheck.com

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L/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-1104 | CWE-1104 CWE-1104 Use of Unmaintained Third-Party Components

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:L/SC:H/SI:H/S
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:L/SC:H/SI:H/S
3.1	disclosure@vulncheck.com	Primary	8.7	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L
3.1	CNA	CVSS	8.7	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L

## CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

Low

Sub Conf.

High

Sub Integrity

High

Sub Availability

Low

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L/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

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

Low

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

### Vendor Declared Affected Products

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

### References

Reference	Source	Link
-----------	--------	------

<a href="https://github.com/kmkz/Exploits/blob/master/2026/CVE-2026-22191-POC.py">github.com/kmkz/Exploits/blob/master/2026/CVE-2026-22191-POC.py</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="https://github.com">github.com</a>
<a href="https://github.com/kmkz/Exploits/blob/master/2026/CVE-2026-22191-SicuroWeb-ATI-c...">github.com/kmkz/Exploits/blob/master/2026/CVE-2026-22191-SicuroWeb-ATI-c...</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="https://github.com">github.com</a>
<a href="https://www.boffsec-services.com/posts/sicuroweb-cve-2026-22191">www.boffsec-services.com/posts/sicuroweb-cve-2026-22191</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="https://www.boffsec-services.com">www.boffsec-services.com</a>
<a href="https://www.vulncheck.com/advisories/beghelli-sicuro24-sicuroweb-angularjs-sandbox-esca...">www.vulncheck.com/advisories/beghelli-sicuro24-sicuroweb-angularjs-sandbox-esca...</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="https://www.vulncheck.com">www.vulncheck.com</a>
<a href="https://www.beghelli.it">www.beghelli.it</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="https://www.beghelli.it">www.beghelli.it</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### 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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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)