Beghelli Sicuro24 SicuroWeb AngularJS Sandbox Escape via Template Injection

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-41468
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 19:17:08 UTC
Updated	2026-04-22 21:18:45 UTC
Description	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/MSC:X/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/MSC: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

github.com/kmkz/Exploits/blob/master/2026/CVE-2026-22191-POC.py	disclosure@vulncheck.com	github.com
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.
www.vulncheck.com/advisories/beghelli-sicuro24-sicuroweb-angularjs-sandbox-esca...	disclosure@vulncheck.com	www.vulncheck.com
www.beghelli.it	disclosure@vulncheck.com	www.beghelli.it
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.