Authorization Bypass Through User-Controlled Key in Crafty Controller

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

Summary

CVE	CVE-2026-5652
State	PUBLISHED
Assigner	GitLab
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 17:16:57 UTC
Updated	2026-04-27 19:47:08 UTC
Description	An insecure direct object reference vulnerability in the Users API component of Crafty Controller allows a remote, authentic

Risk And Classification

Primary CVSS: v3.1 9 CRITICAL from cve@gitlab.com

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

EPSS: 0.000920000 probability, percentile 0.257830000 (date 2026-04-27)

Problem Types: CWE-639 | CWE-639 CWE-639: Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
3.1	cve@gitlab.com	Secondary	9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L
3.1	CNA	CVSS	9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Craftycontrol	Crafty Controller	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Arcadia Technology LLC	Crafty Controller	affected 4.10.2 semver	Not specified

References

Reference	Source	Link	Tags
gitlab.com/crafty-controller/crafty-4/-/work_items/705	134c704f-9b21-4f2e-91b3-4a467353bcc0	gitlab.com	Exploit, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Thank you to [Kacper Leszczyński / szotgan](https://gitlab.com/szotgan) on GitLab for reporting this issue. (en)

Additional Advisory Data

Solutions

CNA: Upgrade to version 4.10.3

There are currently no legacy QID mappings associated with this CVE.

site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report