



Unauthenticated Path Traversal in FalkorDB Browser Leads to Remote Code Execution

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

Summary

CVE	CVE-2026-6057
State	PUBLISHED
Assigner	securin
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 10:16:04 UTC
Updated	2026-04-10 21:16:28 UTC
Description	FalkorDB Browser 1.9.3 contains an unauthenticated path traversal vulnerability in the file upload API that allows remote at

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from ADP

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

EPSS: 0.000890000 probability, percentile 0.254050000 (date 2026-04-10)

Problem Types: CWE-22 | CWE-22 CWE-22 Path Traversal

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	FalkorDB	FalkorDB Browser	affected 1.9.3	Linux, 64 bit, Windows

References

Reference	Source	Link	Tags
github.com/FalkorDB/falkordb-browser	33c584b5-0579-4c06-b2a0-8d8329fcab9c	github.com	
github.com/FalkorDB/falkordb-browser/pull/1611	33c584b5-0579-4c06-b2a0-8d8329fcab9c	github.com	
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: Ramesh Gunnam from Securin (en)

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