

CVE-2023-41266

Qlik Sense Path Traversal Vulnerability

CISA KEV since Dec 7, 2023

Actively exploited

Ransomware use known

A path traversal vulnerability found in Qlik Sense Enterprise for Windows for versions May 2023 Patch 3 and earlier, February 2023 Patch 7 and earlier, November 2022 Patch 10 and earlier, and August 2022 Patch 12 and earlier allows an unauthenticated remote attacker to generate an anonymous session. This allows them to transmit HTTP requests to unauthorized endpoints. This is fixed in August 2023 IR, May 2023 Patch 4, February 2023 Patch 8, November 2022 Patch 11, and August 2022 Patch 13.

EVRS 85 /100 Immediate priority	CVSS V3.1 6.5 Medium · NVD	EPSS 0.848 99.71st percentile · FIRST	CISA DEADLINE Dec 28, 2023 KEV since 2023 · listed over a year
--	---	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.848 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply remediations or mitigations per vendor instructions or discontinue use of the product if remediation or mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
qlik sense	august 2022 february 2023 may 2023 november 2022	no fixed version listed	NVD

Sources

Vendor guidance	community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801	NVD	nvd.nist.gov/vuln/detail/CVE-2023-41266
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-45783
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-41266		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.