



Path Traversal in Diagram

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2026-7182
State	PUBLISHED
Assigner	CERT-PL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 13:16:19 UTC
Updated	2026-05-15 13:16:19 UTC
Description	Diagram's export module is vulnerable to Path Traversal in src attribute due to lack of HTML sanitization. An unauthenticated user can traverse the file system and read arbitrary files.

Risk And Classification

Primary CVSS: v4.0 9.2 CRITICAL from cvd@cert.pl

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N/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-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
4.0	cvd@cert.pl	Secondary	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N/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
4.0	CNA	CVSS	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

None

Sub Availability

None

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

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	DHTMLX	Diagram	affected 1.0.0 1.1.1 semver	Not specified

References			
Reference	Source	Link	Tags
docs.dhtmlx.com/diagram/whats_new	cvd@cert.pl	docs.dhtmlx.com	
cert.pl/en/posts/2026/05/CVE-2026-7182	cvd@cert.pl	cert.pl	
dhtmlx.com/docs/products/dhtmlxDiagram	cvd@cert.pl	dhtmlx.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: Łukasz Jaworski (Pentest Limited) (en)

CNA: Tomasz Holeksa (Pentest Limited) (en)

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

