Remote Code Execution in PDF Export Module

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

Summary

CVE	CVE-2026-41553
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	PDF Export Module used in DHTMLX's products Gantt and Scheduler is vulnerable to Remote Code Execution due to lack

Risk And Classification

Primary CVSS: v4.0 10 CRITICAL from cvd@cert.pl

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
4.0	cvd@cert.pl	Secondary	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/C...
4.0	CNA	CVSS	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	DHTMLX	PDF Export Module	affected 0.3.3 0.7.6 semver	Not specified

References

Reference	Source	Link	Tags
cert.pl/en/posts/2026/05/CVE-2026-7182	cvd@cert.pl	cert.pl	
docs.dhtmlx.com/gantt/guides/pdf-export-module-whatsnew	cvd@cert.pl	docs.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.