Arbitrary File Read and Server Side Request Forgery via XML External Entities in 4D Server SOAP

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

Summary

CVE	CVE-2024-39847
State	PUBLISHED
Assigner	SCHUTZWERK
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 07:16:36 UTC
Updated	2026-04-30 07:16:36 UTC
Description	Unauthenticated attackers can exploit a weakness in the XML parser functionality of the SOAP endpoints in 4D server. This

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from 23637b5d-af4c-4cf9-b8f6-deb7fd0f8423

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:X/V:X/RE:X/U:X

Problem Types: CWE-611 | CWE-611 CWE-611 Improper Restriction of XML External Entity Reference

Version	Source	Type	Score	Severity	Vector
4.0	23637b5d-af4c-4cf9-b8f6-deb7fd0f8423	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

ntegrity

None

Availability

None

Sub Conf.

None

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:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	4D	4D Server	affected * v20 R3 custom	Windows
CNA	4D	4D Server	unknown v20 R4 v20 R6 custom	Windows
CNA	4D	4D Server	unaffected v20 R7 custom	Windows

References

Reference	Source	Link	Tags
4d.com	23637b5d-af4c-4cf9-b8f6-deb7fd0f8423	4d.com	
www.schutzwerk.com/en/blog/schutzwerk-sa-2024-002	23637b5d-af4c-4cf9-b8f6-deb7fd0f8423	www.schutzwerk.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

Vendor Comments And Credit

Discovery Credit

CNA: Marcelo Reyes of SCHUTZWERK GmbH (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-06-17T11:00:00.000Z	Vulnerability discovered
CNA	2024-06-24T11:00:00.000Z	Attempt to contact vendor, no response received
CNA	2024-06-25T11:00:00.000Z	CVE ID requested
CNA	2024-06-29T14:59:00.000Z	CVE-2024-39847 assigned
CNA	2024-07-04T11:00:00.000Z	Attempt to contact vendor again, no response received

CNA	2024-07-04T11:00:00.000Z	Attempt to contact vendor again, no response received
CNA	2024-07-09T11:00:00.000Z	Attempt to contact vendor again, no response received
CNA	2024-07-16T11:00:00.000Z	Attempt to contact vendor again, no response received
CNA	2024-07-22T11:00:00.000Z	Attempt to contact vendor again, no response received
CNA	2026-04-29T11:00:00.000Z	Advisory published

Solutions

CNA: Update to 4D Server 20 R7 or higher.

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