Stored Cross-Site Scripting (XSS) Vulnerability in Design Name

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

Summary

CVE	CVE-2026-4345
State	PUBLISHED
Assigner	autodesk
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 15:16:38 UTC
Updated	2026-04-22 15:04:58 UTC
Description	A maliciously crafted HTML payload, stored in a design name and exported to CSV, can trigger a Stored Cross-site Scriptin

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from psirt@autodesk.com

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

EPSS: 0.000240000 probability, percentile 0.064710000 (date 2026-04-21)

Problem Types: CWE-79 | CWE-79 CWE-79 Cross-Site Scripting (XSS) - Stored

Version	Source	Type	Score	Severity	Vector
3.1	psirt@autodesk.com	Secondary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

High

vailability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Autodesk	Fusion	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Autodesk	Fusion	affected 2606.0 2702.1.47 custom	Not specified

References

Reference	Source	Link
dl.appstreaming.autodesk.com/production/installers/Fusion%20Client%20Downloader.exe	psirt@autodesk.com	dl.appstreaming.autodes
dl.appstreaming.autodesk.com/production/installers/Fusion%20Client%20Downloader.dmg	psirt@autodesk.com	dl.appstreaming.autodes
www.autodesk.com/trust/security-advisories/adsk-sa-2026-0005	psirt@autodesk.com	www.autodesk.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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