



CVE-2022-47636

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-47636
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-10 16:15:00 UTC
Updated	2023-08-17 21:26:00 UTC
Description	A DLL hijacking vulnerability has been discovered in OutSystems Service Studio 11 11.53.30 build 61739. When a user opens a project in Service Studio, the application will attempt to load the DLLs specified in the project's configuration. If a malicious actor can manipulate the configuration to point to a malicious DLL, they can execute arbitrary code on the user's machine.

Risk And Classification

Problem Types: CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Outsystems	Service Studio	11.53.30	All	All	All

References

Reference	Source	Link	Tags
OutSystems Service Studio 11.53.30 - DLL Hijacking - Windows local Exploit	MISC	www.exploit-db.com	
OutSystems Service Studio 11.53.30 DLL Hijacking ~ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report