



CVE-2022-36263

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

Summary

CVE	CVE-2022-36263
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-19 15:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	StreamLabs Desktop Application 1.9.0 is vulnerable to Incorrect Access Control via obs64.exe. An attacker can execute art

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Logitech	Streamlabs Desktop	1.9.0	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference	Source	Link	Tags
Vuln/Streamlabs-CreateProcessW-API-Misuse-Binary-Hijack at main · ycdxsb/Vuln · GitHub	MISC	github.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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)