



CVE-2023-27054

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

Summary

CVE	CVE-2023-27054
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-22 22:15:00 UTC
Updated	2023-03-28 19:48:00 UTC
Description	A cross-site scripting (XSS) vulnerability in MiroTalk P2P before commit f535b35 allows attackers to execute arbitrary web s

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mirotalk	Mirotalk P2p	All	All	All	All

References

Reference
GitHub - mirosлавpejic85/mirotalk: ???? WebRTC - P2P - Simple, Secure, Fast Real-Time Video Conferences Up to 4k and 60fps, compatible
[mirotalk] - #139 prevent XSS through DC · mirosлавpejic85/mirotalk@f535b35 · GitHub
Multiple Cross-Site Scripting (XSS) · Issue #139 · mirosлавpejic85/mirotalk · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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