

OFFENSIVE SECURITY

Schwachstellen in Videokonferenzsystemen

Schwachstellen in MiroTalk entdeckt und behoben. Erfahren Sie mehr über die

Datenschutz ist unser Kerngeschäft

Als Cybersecurity-Unternehmen nehmen wir den Schutz Ihrer Daten besonders ernst. Reichweitenmessung läuft cookielos über Matomo, selbst gehostet in Deutschland – ohne Drittanbieter und ohne Ihre Zustimmung zu benötigen. Marketing-Cookies messen optional die Wirksamkeit unserer Anzeigen über Google Ads (Datentransfer in die USA, EU-US Data Privacy Framework). Details finden Sie in unserer [Datenschutzerklärung](#).

ISO 27001

ISO 9001

IT SECURITY MADE IN GERMANY

Alle akzeptieren

Alle ablehnen

Einstellungen

Videokonferenzsystem MiroTalk: fehlende Zugriffskontrolle beim Entfernen von Meeting-Teilnehmern (CVE-2024-44729), Chat-Manipulation mit gefälschtem Absender (CVE-2024-44730), DOM-basiertes XSS über Chat-Nachrichten (CVE-2024-44731) und unbefugtes Ändern von Benutzernamen (CVE-2024-44734). Alle Schwachstellen wurden dem Entwickler sofort gemeldet, bestätigt und innerhalb weniger Tage behoben.

Diese Zusammenfassung wurde KI-gestützt erstellt (EU AI Act Art. 50).

► Inhaltsverzeichnis (6 Abschnitte)

Videokonferenzsysteme sind spätestens nach Corona ein fester Bestandteil des Arbeitslebens. Neben bekannten Vertretern wie Zoom, Microsoft Teams und Google

Meet, finden auch Open-Source Varianten wie BigBlueButton mehr Bekanntheit. Open-Source-Software bieten die Vorteile der eigenen Datenhoheit und öffentlich zugänglichen Quellcode, der es Sicherheitsforschern erlaubt eine Quellcode-Analyse durchzuführen, um die Projekte sicherer zu machen.

01 Schwachstellen bei MiroTalk

Eines der Open-Source Videokonferenzsysteme ist MiroTalk. MiroTalk präsentiert sich als [Open-Source](#) WebRTC-basierte Plattform, die es Teilnehmern ermöglicht in Echtzeit über Peer-to-Peer (P2P) Videokonferenzen abzuhalten. Dabei werden besonders die Merkmale "Einfachheit, Sicherheit und Geschwindigkeit" hervorgehoben. Zusätzlich unterstützt MiroTalk viele Features, wie zum Beispiel Screensharing, die Nutzung von Whiteboards und verschlüsselte Videoanrufe.

Das Projekt hat, Stand Oktober 2024, 3.000 Sterne auf GitHub und ist somit recht populär. Es werden auch andere Versionen angeboten, wie z.B. MiroTalk SFU (Selective Forwarding Unit),

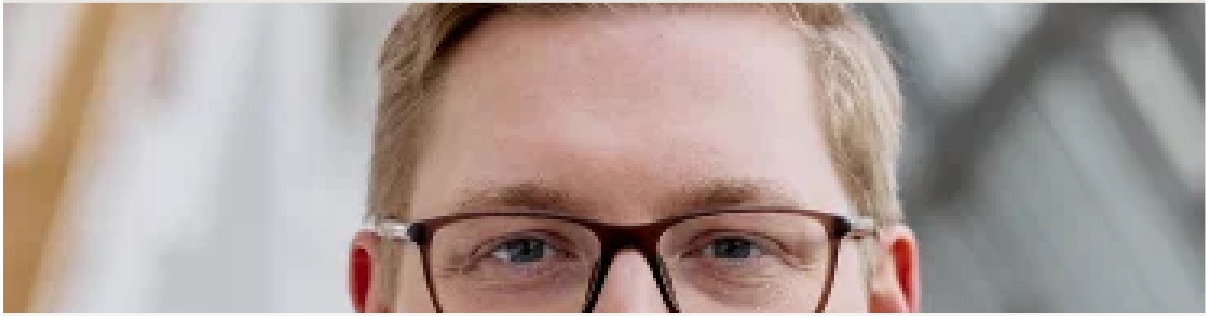
Datenschutz ist unser Kerngeschäft

Als Cybersecurity-Unternehmen nehmen wir den Schutz Ihrer Daten besonders ernst. Reichweitenmessung läuft cookielos über Matomo, selbst gehostet in Deutschland — ohne Drittanbieter und ohne Ihre Zustimmung zu benötigen. Marketing-Cookies messen optional die Wirksamkeit unserer Anzeigen über Google Ads (Datentransfer in die USA, EU-US Data Privacy Framework). Details finden Sie in unserer [Datenschutzerklärung](#).

ISO 27001 ISO 9001 IT SECURITY MADE IN GERMANY

Behobene Version: [Commit \[9de226\]](#) (April 22, 2023)

Die erste Schwachstelle erlaubt es durch fehlende Zugriffskontrolle das Entfernen von beliebigen Nutzern aus beliebigen Meetings. Das Entfernen von Teilnehmern ist ein essenzielles Sicherheitsfeature in Videokonferenzsystemen. Es sollte aber nur höher privilegierten Teilnehmern zur Verfügung stehen, andere Teilnehmer zu entfernen. Jedoch kann ein Angreifer, welcher nicht Teil des Meetings sein muss, beliebige Teilnehmer aus beliebigen Meetings entfernen. Der Angreifer muss nur die Peer ID des jeweiligen Nutzers kennen und eine WebSocket-Verbindung zum Server haben. Alle Peer IDs sind Meeting-Teilnehmern bekannt. Somit kann ein Angreifer, der im Meeting war und entfernt wurde, alle Teilnehmer hinauswerfen. Eine alternative Möglichkeit ist alle Teilnehmer auf einmal zu entfernen. Dafür muss nur die Room ID bekannt sein. Das führt dazu, dass Meetings unterbrochen werden oder nicht stattfinden können.



Monatlicher Threat Report

Chris Wojzechowski bewertet einmal im Monat die aktuelle Bedrohungslage aus Sicht eines Informationssicherheitsexperten. Sein 30-köpfiges Team ist näher an realen Cyberbedrohungen dran als kaum jemand sonst - mit konkreten Handlungsempfehlungen, die Sie am nächsten Morgen umsetzen können.

Bestseller-Autor (Wiley-VCH) · M.Sc. Internet-Sicherheit · Bekannt aus Handelsblatt & WamS

Datenschutz ist unser Kerngeschäft

Als Cybersecurity-Unternehmen nehmen wir den Schutz Ihrer Daten besonders ernst. Reichweitenmessung läuft cookielos über Matomo, selbst gehostet in Deutschland – ohne Drittanbieter und ohne Ihre Zustimmung zu benötigen. Marketing-Cookies messen optional die Wirksamkeit unserer Anzeigen über Google Ads (Datentransfer in die USA, EU-US Data Privacy Framework). Details finden Sie in unserer [Datenschutzerklärung](#).

ISO 27001

ISO 9001

IT SECURITY MADE IN GERMANY

An

Behobene Version: [Commit \[c21d58\]](#) (April 25, 2023)

Die anfällige Version erlaubt es Angreifern Chat-Nachrichten zu manipulieren. Das führt zu einer Vielzahl von Angriffen. CVE-2024-44730 beschreibt einen Angriff, der es einem Angreifer erlaubt Nachrichten zu verfassen und einen beliebigen Absender anzugeben. Der Server ist bei Chat-Nachrichten nicht beteiligt, da der Chat über RTC funktioniert. Somit kommunizieren die Browser bei Chat-Nachrichten untereinander und müssen clientseitig die Identitäten der Nutzer sicherstellen. Somit muss der Angreifer im Meeting sein, damit eine RTC-Verbindung zu den anderen Browsern hergestellt ist.

04 CVE-2024-44731

Anfällige Version: [Commit \[3440a6a\]](#) (April 13, 2023) **Behobene Version:** [Commit \[9de226\]](#) (April 22, 2023)


CVE-2024-44731 beschreibt ebenfalls eine Chat-Manipulation, die zu einer DOM XSS-Schwachstelle führt. Die Nachricht wird direkt über die RPC-Verbindung an die anderen Teilnehmer gesendet und der Angreifer-Code wird beim Einfügen in den DOM ausgeführt. Falls der Angreifer den Code nicht eintippen möchte, kann auch das Speech-to-Text-Feature genutzt werden, um den Schadcode an Teilnehmer zu senden. Die Auswirkungen sind abhängig von dem Payload, den der Angreifer nutzt. Der Angreifer könnte auf die WebRTC-Einstellungen anderer Teilnehmer zugreifen. Da der Angreifer eine RTC-Verbindung aufgebaut haben muss, muss der Angreifer im Meeting sein.

05 CVE-2024-44734

Anfällige Version: [Commit \[3440a6a\]](#) (April 13, 2023)

Behobene Version: [Commit \[9de226\]](#) (April 22, 2023)

CVE-44733 ermöglicht das Ändern von Benutzernamen anderer Nutzer und des eigenen auf

A screenshot of a website's privacy policy page. The page has a dark blue background with white text. At the top, it says "Datenschutz ist unser Kerngeschäft". Below that, it states "Als Cybersecurity-Unternehmen nehmen wir den Schutz Ihrer Daten besonders ernst." and "Reichweitenmessung läuft cookielos über Matomo, selbst gehostet in Deutschland — ohne Drittanbieter und ohne Ihre Zustimmung zu benötigen." It also mentions "Marketing-Cookies messen optional die Wirksamkeit unserer Anzeigen über Google Ads (Datentransfer in die USA, EU-US Data Privacy Framework)". At the bottom, there are three circular icons: "ISO 27001", "ISO 9001", and "IT SECURITY MADE IN GERMANY". The screenshot is partially obscured by a dark blue overlay.

einer anderen Person im Meeting annehmen kann und sich somit als eine andere Person ausgeben kann. Für diese Variante braucht der Angreifer ebenfalls nur die Room ID und den Namen des Nutzers.

06 Gemeinsam gegen Schwachstellen

Transparenz und Sicherheit sind einige wichtige Aspekte von Open-Source-Software. Diese Aspekte sind jedoch nur gegeben, wenn Sicherheitsforscher die Software auch analysieren. Wir freuen uns der Open-Source-Community etwas zurückzugeben, indem wir die Software auf Schwachstellen untersuchen.

Wir danken dem Entwickler Miroslav Pejč für die schnelle Antwort und die angenehme Zusammenarbeit.

Nächster Schritt

Unsere zertifizierten Sicherheitsexperten beraten Sie zu den Themen aus diesem Artikel – unverbindlich und kostenlos.

[Kostenlose Erstberatung vereinbaren](#)

[Leistungen ansehen](#)

Kostenlos · 30 Minuten · Unverbindlich

ARTIKEL TEILEN

<https://www.linkedin.com/sharing/share-offsite?url=https%3A%2F%2Fwww.a7.de%2Fblog%2Fschwachstellen-in-videokonferenzsystemen/>

<https://x.com/intent/post?url=https%3A%2F%2Fwww.a7.de%2Fblog%2Fschwachstellen-in-videokonferenzsystemen/>

Link

E-

Datenschutz ist unser Kerngeschäft

Als Cybersecurity-Unternehmen nehmen wir den Schutz Ihrer Daten besonders ernst. Reichweitenmessung läuft cookielos über Matomo, selbst gehostet in Deutschland – ohne Drittanbieter und ohne Ihre Zustimmung zu benötigen. Marketing-Cookies messen optional die Wirksamkeit unserer Anzeigen über Google Ads (Datentransfer in die USA, EU-US Data Privacy Framework). Details finden Sie in unserer [Datenschutzerklärung](#).

ISO 27001

ISO 9001

IT SECURITY MADE IN GERMANY

[WLAN-Penetrationstest: Tools, Methoden und Angriffsvektoren](#)

[Chris Wojzechowski](#) : [14 Min.](#)

[Active Directory absichern: 15 Maßnahmen gegen die häufigsten...](#)

[Vincent Heinen](#) : [11 Min.](#)

OFFENSIVE SECURITY

[Active Directory Red Team: Kerberoasting, Golden Ticket und...](#)

[Vincent Heinen](#) : [12 Min.](#)