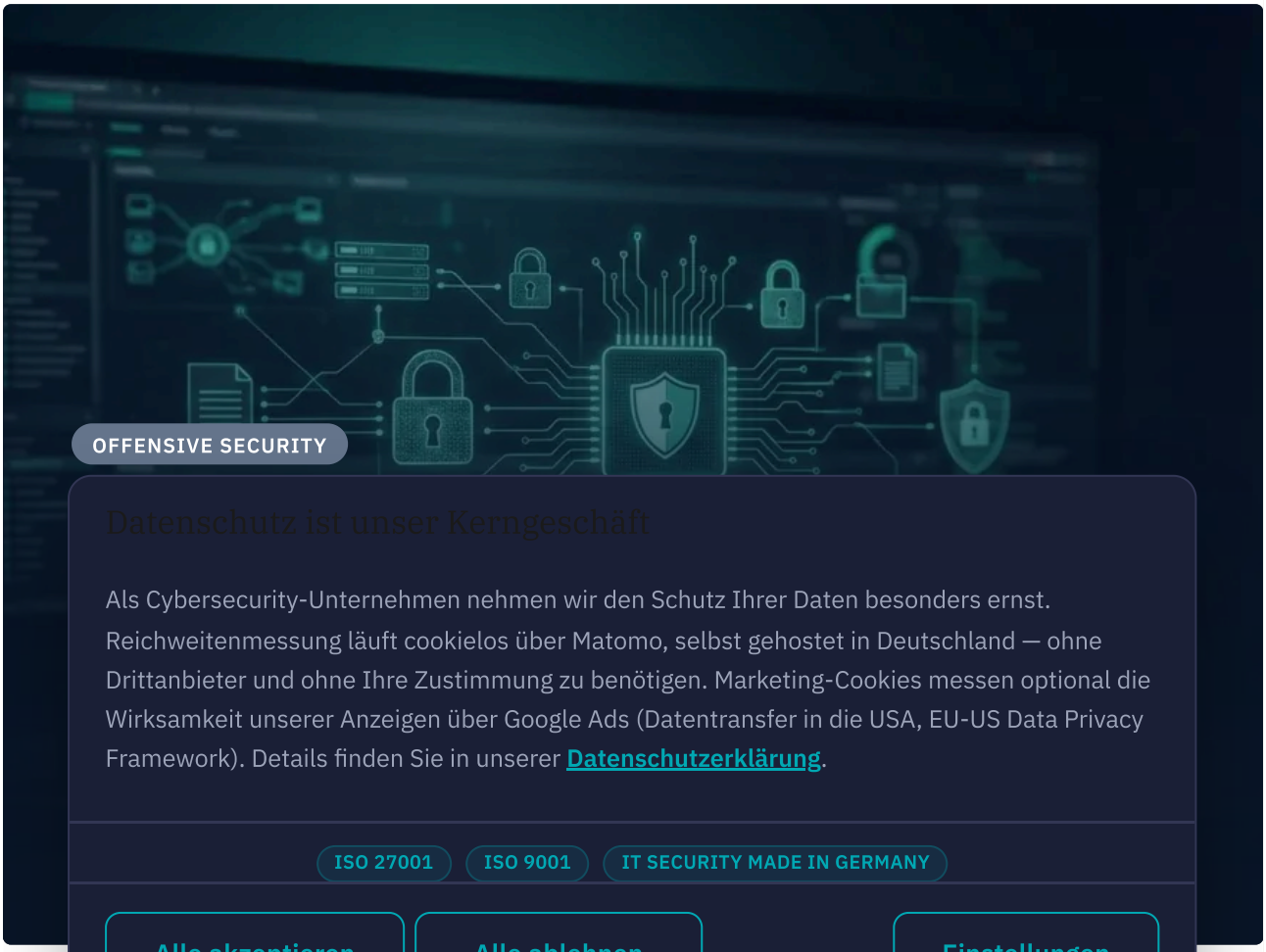

TL;DR

AWARE7 entdeckte im April 2023 vier Schwachstellen im Open-Source-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.

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

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.

03 CVE-2024-44730

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

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

Die zweite Variante ist das Ändern des eigenen Namens. Bevor man den eigenen Namen ändert, wird eine Anfrage an den Server gestellt, wo geprüft wird, ob der Name bereits existiert. Die Funktion der Prüfung des Namens lässt sich überschreiben und führt dazu, dass den Namen 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 Pejc für die schnelle Antwort und die angenehme Zusammenarbeit.

Weitere Artikel aus Offensive Security

OFFENSIVE SECURITY

WLAN-Penetrationstest: Tools, Methoden und Angriffsvektoren

Chris Wojzechowski · 14 Min.

OFFENSIVE SECURITY

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.