PRESSEMITTEILUNG
Auctores GmbH

Neumarkt, den 09.07.2021

Sicherheitslücke bei Visavid erkannt und geschlossen

Expertin konnte Warteraum des Videokonferenz-Systems überwinden und unbemerkt teilnehmen

Eine externe Sicherheitsforscherin hat der Auctores GmbH eine mögliche Sicherheitslücke im von Auctores entwickelten Videokonferenz-System Visavid gemeldet. Das Problem wurde durch ein Update bereits behoben. Die zuständigen Fachstellen (Bayern-CERT und BayLDA) wurden unterrichtet, Auctores steht im direkten Austausch mit den Behörden. Nach derzeitigem Stand geht das BAyLDA von einem geringen Datenschutzrisiko aus.

Bei der potenziellen Sicherheitslücke war es versierten Angreifer*innen mit entsprechender krimineller Energie möglich, einen Raum trotz aktivierten Warteraums ohne Freigabe durch Moderator*innen zu betreten. Für einen normalen Nutzer war dies nicht möglich. Lilith Wittmann, die die Lücke entdeckt hat, hatte dabei zunächst einen Visavid-Konferenzraum über einen gültigen Zugangslink betreten und dann den Raum von innen technisch analysiert. Nach dem Entdecken des Problems informierte sie das Auctores-Team, das die Lücke unmittelbar schloss.

Auctores sieht die entdeckte Sicherheitslücke als kritisch an. Wittmann konnte aufgrund ihrer Analyse bei einer durch den Warteraummechanismus geschützten Videokonferenz Zugang nur mithilfe der Raum-ID erlangen. Dabei nutzte sie den Token-Vergabemechanismus, der einen Nutzer-Token ausstellte, bevor die Moderator*in die Nutzer*in zu einer Konferenz zugelassen hat. Mit diesem Token konnte sie sich mit dem Websocket des Videokonferenz-Koordinationsservers verbinden, dort die Liste der Teilnehmenden anfragen und die Tokens zum Versenden und Empfangen von Videostreams abrufen.

Eine potenzielle böswillige Angreifer*in konnte damit den Warteraummechanismus umgehen und unbemerkt Audio- und Videostreams der Teilnehmer empfangen und somit letztlich auch lokal aufzeichnen. Außerdem konnte die Angreifer*in als Sprecher*in dem Audiokanal beitreten, ohne im Raum sichtbar zu sein, Chat-Nachrichten in die Runde und 1:1 senden, wenn diese Funktionen für Teilnehmer*innen freigegeben waren, die Funktion „Hand heben“ nutzen und unbemerkt Dateien und Whiteboards herunterladen.

Eine Angreifer*in konnte nicht am Warteraum vorbei als normale Teilnehmer*in in der Sitzung angezeigt werden, dies war nur mit Bestätigung durch eine Moderator*in möglich. Sie konnte auch nicht ein für andere Teilnehmer*innen sichtbares Video in den Raum einschleusen. Die Visavid-Räume lassen sich grundsätzlich durch einen Einwahlcode schützen. Bei aktivem Einwahlcode war der hier demonstrierte Angriff nicht möglich.

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) geht nach bisherigem Stand von einer „geringen Eintrittswahrscheinlichkeit eines Datenschutzrisikos“ aus, da neben der „White-Hat-Hackerin“ keine weiteren Personen unbefugt auf Räume des Visavid-Systems zugegriffen haben. Unter diesen Voraussetzungen sieht das BayLDA kein hohes Risiko nach Art. 34 DS-GVO mit der Verpflichtung der Verantwortlichen, die Betroffenen zu informieren.

Auctores GmbH
Amberger Straße 82
92318 Neumarkt

Geschäftsführer Karl Weigl
HRB 22474 AG Nürnberg
Steuernr. 201/121/80529
USt.-Id. DE248382991

Telefon: +49 9181 5198-0
Telefax: +49 9181 5198-200
E-Mail: info@auctores.de
Web: www.auctores.de

Da Visavid in bayerischen Schulen eingesetzt wird, sind auch das Landesamt für Sicherheit in der Informationstechnik (LSI) und der Bayerische Landesbeauftragte für Datenschutz informiert worden. Aktuell führt Auctores noch weitere Untersuchungen durch, um sicherzustellen, dass es keinen Datenabfluss gegeben hat.

Um die entdeckte Lücke auszunutzen, hätten Angreifer*innen nicht nur entsprechende technische Kenntnisse benötigt, sondern auch die URL des Raums kennen müssen. Für Videokonferenz-Räume erzeugt Visavid grundsätzlich eine zufällige, nicht erratbare und nicht „hochzählbare“ URL, bei personalisierten Einladungen einschließlich codierter, nutzerspezifischer Kennung. Diese URL ist für Suchmaschinen nicht unmittelbar über die Website auffindbar, weil es keinen verfolgbaren Pfad dorthin gibt. Ein Suchmaschinenbot kann also nicht von sich aus auf die URL des Raums kommen. Die Räume selbst sind außerdem per Meta-Angabe „noindex, nofollow“ für Suchmaschinen gesperrt, erscheinen also nicht direkt auf den Ergebnisseiten von Suchmaschinen, die sich – wie Google oder Bing – an diese Meta-Angaben halten.

Räume sind allerdings auffindbar, wenn die Links zu ihnen öffentlich verbreitet werden. Werden also Links zu Visavid-Räumen entgegen den Nutzungsbedingungen und Sicherheitshinweisen offen sichtbar etwa auf Schul-Websites gepostet, kann jeder Besucher der Website einschließlich Suchmaschinenroboter den Link aufrufen. Suchmaschinenbots lesen natürlich nicht nur den mehr oder weniger verräterischen Linktext, sondern auch die eigentliche URL und nehmen diese dann in den Index auf. Dieses Problem lässt sich allerdings nicht auf technischem Weg lösen, sondern nur über Sensibilisierung von Veranstaltern und Anwendern – ebenso wie bei der empfohlenen Nutzung des Einwahlcodes als zusätzliche Sicherheitsmaßnahme.

Die Sicherheit von Visavid war vor der Freigabe für den Einsatz an bayerischen Schulen durch mehrere Penetrationstests überprüft worden. Dafür hatte Auctores zwei darauf spezialisierte Unternehmen beauftragt, ein weiteres Unternehmen war im Auftrag des bayerischen Kultusministeriums tätig geworden.

Hinweis: Pressemitteilungen im Word- und PDF-Format sowie Fotos in druckfähiger Auflösung finden Sie unter https://visavid.de/presse.

Über Auctores:

Die Auctores GmbH baut auf mehr als zwei Jahrzehnte personelle und technische Erfahrung im E-Business. Bereits 1998 als Abteilung eines Computer-Systemhauses gegründet, wurde sie Anfang 2006 als GmbH ausgegründet und vom jetzigen Geschäftsführer Karl Weigl übernommen und konsequent ausgebaut. Auctores entwickelt marktorientierte, medienübergreifende Kommunikations- und Software-Strategien. Einen Schwerpunkt bilden webbasierte Anwendungen für eine Vielzahl von Geschäftsprozessen. Darüber hinaus übernimmt Auctores als Cross-Media-Agentur auch die redaktionelle Betreuung ein-schließlich Fachredaktion und medien- und zielgruppengerechter Aufbereitung sowie Produktion. Für Cross-Media-Anwendungen und -Produkte stellt sie die Infrastruktur bereit. Auctores entwickelt digitale Geschäftsmodelle und ist in den Bereichen Kommunikation, Marketing und Corporate Design aktiv. Neben den Stammsitz in Neumarkt i. d. OPf. hat Auctores einen Standort in Frankfurt/Main.

Kontakt:

Auctores GmbH
Amberger Straße 82
92318 Neumarkt

Tel.: 09181 5198-0
Fax: 09181 5198-200
E-Mail: presse@auctores.de