Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Webex by Cisco: Schwachstelle ermöglicht Abfluss von Metadaten

CSW-Nr. 2024-248744-10k2, Version 1.0, 10.06.2024

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Webex by Cisco ist ein Kommunikations- und Kolaborationstool welches vor allem für Videokonferenzen genutzt wird. Journalisten und Sicherheitsforschende haben darin eine Sicherheitslücke aufgedeckt Cisco darüber informiert und den Sachverhalt veröffentlicht [ZEIT24], [NETZ24]. Daraufhin hat Cisco am 04.06.2024 ein Advisory veröffentlicht und den Sachverhalt grundsätzlich bestätigt [CISC24a]. Die Sicherheitslücke erlaubte es auf Metadaten des Meetings zuzugreifen und durch Enummeration weitere Meetings zu identifizieren. In Kombination mit unsicher konfigurierten, insbesondere nicht mit einem Passwort geschützten Meetings, konnten sich die Sicherheitsforschenden unautorisiert in einige dieser Meetings einwählen.

Nach derzeitigem Kenntnisstand waren die folgenden Metadaten zugänglich:

- Meeting-UUID (universally Unique IDentifier)
- Nummer des Meetings
- Titel des Meetings
- Name des Hosts
- Datum und Uhrzeit des geplanten Meetings
- Geplante Dauer des Meetings

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb: IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange: Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Dagegen waren nach derzeitigem Kenntnisstand die folgenden Metadaten NICHT zugänglich:

- Passwort des Meetings
- Informationen über Teilnehmer des Meetings

Das BSI hat den Abfluss der Metadaten als Datenschutzverletzung an den BfDI gemeldet. Auch im europäischen Ausland, wie z.B. die Niederlande, waren Organisationen von der Schwachstelle betroffen [NIEU24].

Die Sicherheitslücke ist laut Cisco seit dem 28.05.2024 behoben [CISC24a]. Cisco hat gemäß eigener Aussage die Kunden über die erkannten Ausnutzungen informiert. Nach Erkenntnissen des BSI sind allerdings nicht alle potentiell betroffenen Kunden informiert worden, und die Informationen waren auch nicht vollständig.

Nach derzeitigem Kenntnisstand sind zukünftige, neu aufgesetzte Meetings nicht mehr gefährdet. Es ist jedoch möglich, dass vor dem Beheben durch Cisco angelegte - noch ausstehende - Meetings weiterhin aufgeklärt werden können.

Bewertung

Kommunikationstools sind für Angreifer ausgesprochen interessante Ziele, da sie neben den besprochenen Fakten, tiefe Einblicke in die Organisation, Bewertungen, Hintergründe und Zusammenhänge gewähren.

Derzeit liegen dem BSI keine Erkenntnisse vor, dass die Sicherheitslücke außer von den Sicherheitsforschern auch noch von weiteren potentiellen Angreifenden ausgenutzt wurde.

Die Sicherheitslücke hat, wenn man sich an die Empfehlungen des BSI gehalten hat, "nur" zum Abfluss von Metadaten geführt. Weil aber einige Meetings ohne ein Passwort angesetzt wurden, konnten die Sicherheitsforschenden sich hier auch einwählen.

Maßnahmen

Cisco hat zentrale Maßnahmen ergriffen. Endnutzer müssen keine Sicherheitsupdates installieren.

Das BSI empfiehlt jedoch grundsätzlich angemessen absichernde Videokonferenzdienste zu nutzen [BSI21]. Cisco stellt für das Produkt Webex die beiden Anleitungen zur Verfügung:

- Best practices for secure meetings: hosts [CISC24b]
- Webex best practices for secure meetings: Control Hub [CISC24c]

Insbesondere sollte(n) [BSI21] [NCSC24]:

- immer Passwörter / PINs genutzt werden
- die Zugangsdaten vorab nur mit berechtigten Personen geteilt werden
- eine Wartelobby eingerichtet sein
- soweit organisatorisch möglich, Teilnehmer vor Beitritt identifiziert werden.

Um sicherzustellen, dass bereits angelegter Meetings nicht gefährdet sind, empfiehlt das BSI **alle bereits angelegten, aber noch ausstehenden Termine zu löschen und neu anzulegen**. Dazu zählen insbesondere bereits **vor dem 28.05.2024 angelegte Regeltermine**. In Einzelfällen kann diese Maßnahme von Cisco für die gesamte Organisation realisiert werden. Dazu sollte der Lieferant kontaktiert werden [NCSC24].

Links

[ZEIT24] Mithören, wenn Beamte sprechen https://www.zeit.de/digital/datenschutz/2024-06/webex-sicherheitsluecke-ministerien-cybersicherheit-it

[NETZ24] Netzbegrünung findet Schwachstellen auch im Cisco WebEx Clouddienst – Behörden und Unternehmen in ganz Europa betroffen https://netzbegruenung.de/blog/netzbegruenung-findet-schwachstellen-auch-im-cisco-webex-clouddienst-behoerden-und-unternehmen-in-ganz-europa-betroffen/

[NIEU24] Gaten in beveiliging videocalls ministers: vergaderinformatie in te zien https://nos.nl/nieuwsuur/artikel/2523301-gaten-in-beveiliging-videocalls-ministers-vergaderinformatie-in-te-zien

[CISC24a] Cisco Webex Meetings Meeting Information and Metadata Issue June 2024 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-june-2024

[BSI21] Mindeststandard des BSI für Videokonferenzdienste https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Videokonferenzdienste/Videokonferenzdienste_node.html

[CISC24b] Best practices for secure meetings: hosts https://help.webex.com/en-us/article/8zi8tq/Best-practices-for-secure-meetings:-hosts

[CISC24c] Webex best practices for secure meetings: Control Hub https://help.webex.com/en-us/article/ov50hy/Webex-best-practices-for-secure-meetings:-Control-Hub

[NCSC24] Meerdere kwetsbaarheden in Cisco Webex https://www.ncsc.nl/actueel/nieuws/2024/juni/07/meerdere-kwetsbaarheden-in-cisco-webex

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1. Was ist das Traffic Light Protokoll?
   Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
2. Welche Einstufungen existieren?
   - **TLP:CLEAR: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
     Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
     - **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
       Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.
3. Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
4. Was passiert, wenn ich die Einstufung nicht beachte?
   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.