Si vous ne visualisez pas ce message, cliquez ici.

ALERTE CYBERSÉCURITÉ

Failles de sécurité critiques dans Zimbra

Date de l'alerte : 23/08/2022

Risques

Vol, voire destruction, de vos données suite à la prise de contrôle à distance de vos équipements.

Description

Deux **failles de sécurité critiques** ont été corrigées dans la solution de messagerie et de collaboration **Zimbra Collaboration**. Elles peuvent être exploitées pour compromettre un système vulnérable sans besoin d'authentification.

L'exploitation de ces failles de sécurité par une personne malveillante peut permettre la prise de contrôle à distance des équipements concernés et le vol, voire la destruction d'informations confidentielles par des cybercriminels.

Des attaques en cours exploitant ces failles de sécurité ont été constatées.

Systèmes concernés

- **Zimbra Collaboration versions 8.8.15 (Joule)** ne disposant pas du correctif de sécurité "Patch 33"
- **Zimbra Collaboration versions 9.0.0 (Kepler)** ne disposant pas du correctif de sécurité "Patch 26"

Mesures à prendre

Il est conseillé de vous rapprocher de vos équipes et/ou prestataires informatique afin de vous assurer que vous ne disposez pas de cette solution ou que vous disposez d'une version non vulnérable.

Si vous disposez d'une version vulnérable du logiciel, nous vous invitons à **mettre à jour au plus vite les équipements concernés** avec les correctifs de sécurité mis à disposition par Zimbra.

Procédure

Se référer aux bulletins de sécurité de l'éditeur pour obtenir les correctifs (en anglais) :

- **Zimbra Collaboration versions 8.8.15 (Joule)** : https://wiki.zimbra.com/index.php/Zimbra_Releases/8.8.15/P33

- **Zimbra Collaboration versions 9.0.0 (Kepler)** : https://wiki.zimbra.com/index.php/Zimbra_Releases/9.0.0/P26

Besoin d'assistance ?

Vous pouvez trouver sur Cybermalveillance.gouv.fr des prestataires de proximité susceptibles de vous apporter leur soutien dans la mise en œuvre de ces mesures : ici.

Références

- ANSSI / CERT-FR :
  - CERTFR-2022-ACT-036
  - CERTFR-2022-AVI-291
  - CERTFR-2022-AVI-736
- CVE-2022-27925
- CVE-2022-37042

Aller plus loin avec Cybermalveillance.gouv.fr :
Pourquoi et comment bien gérer ses mises à jour ?

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

ANSSI