

# ALERTE CYBERSÉCURITÉ



## Faille de sécurité critique dans les produits Windows et Windows Server (Follina)

---

Date de l'alerte : 21/06/2022

### Risques

Espionnage, vol, voire destruction de vos données suite à la prise de contrôle à distance de vos ordinateurs ou serveurs concernés.

### Description

Une **faille de sécurité critique**, baptisée Follina, a été corrigée dans les systèmes d'exploitation **Microsoft Windows et Windows Server**. Cette vulnérabilité peut être exploitée suite à l'ouverture d'un document Word ou au format RTF piégé, y compris lorsque les macros sont désactivées.

L'exploitation de cette faille 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 cette faille de sécurité auraient été constatées.**

### Systemes concernés

- **Windows 7, 8.1, 10 et 11**
- **Windows RT 8.1**
- **Windows Server 2008, 2012, 2016, 2019, 2022 et 20H2**

### Mesure à prendre

**Mettre à jour au plus vite les équipements concernés** avec les correctifs de sécurité mis à disposition par Microsoft.

### Procédure

- Pour **Windows 7, 8.1, 10 et 11** : [support.microsoft.com](https://support.microsoft.com)

### Besoin d'assistance ?

Vous pouvez trouver sur [Cybermalveillance.gouv.fr](https://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 : <https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-005/>
- CVE-2022-30190 (Follina)

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

