Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

S . G . D . S . N
Agence nationale
de la sécurité des
systèmes d'information

Paris, le 16 septembre 2022
N° CERTFR-2022-ALE-007

Affaire suivie par: CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet: Multiples vulnérabilités dans Microsoft Windows

Gestion du document

Référence	CERTFR-2022-ALE-007
Titre	Multiples vulnérabilités dans Microsoft Windows
Date de la première version	16 septembre 2022
Date de la dernière version	16 septembre 2022
Source(s)	Bulletin de sécurité Microsoft CVE-2022-34718 du 13 septembre 2022 Bulletin de sécurité Microsoft CVE-2022-34721 du 13 septembre 2022 Bulletin de sécurité Microsoft CVE-2022-34722 du 13 septembre 2022
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

Risque(s)

- Exécution de code arbitraire à distance

Systèmes affectés

- Windows 10 for 32-bit Systems

- Windows 10 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for x64-based Systems
- Windows 10 Version 21H1 for 32-bit Systems
- Windows 10 Version 21H1 for ARM64-based Systems
- Windows 10 Version 21H1 for x64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 11 for ARM64-based Systems
- Windows 11 for x64-based Systems
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows 8.1 for 32-bit systems
- Windows 8.1 for x64-based systems
- Windows RT 8.1
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server 2022
- Windows Server 2022 Azure Edition Core Hotpatch
- Windows Server 2022 (Server Core installation)

Résumé

Dans le cadre de son *Patch Tuesday*, en date du 13 septembre 2022, Microsoft a indiqué l'existence de multiples vulnérabilités au sein de plusieurs versions de Windows. Trois d'entre elles doivent faire l'objet d'une attention particulière car considérées comme critiques. Elles possèdent un score CVSSv3 de 9.8 et sont respectivement référencées par les numéros suivants : CVE-2022-34718, CVE-2022-34721 et CVE-2022-34722.

La vulnérabilité CVE-2022-34718 permet à un attaquant non authentifié d'envoyer un paquet IPv6 spécialement conçu à destination d'un nœud Windows, provoquant une exécution de code arbitraire à distance.

Les vulnérabilités CVE-2022-34721 et CVE-2022-34722 affectent les extensions du protocole Windows Internet Key Exchange (IKE). Elles permettent à un attaquant non authentifié de provoquer une exécution de code arbitraire à distance. D'après l'éditeur, bien que ces deux vulnérabilités n'affectent que le protocole IKEv1, tous les serveurs Windows seraient concernés car ils acceptent par défaut les paquets des versions 1 et 2.

Par ailleurs, il est à noter que Microsoft a également mis à disposition des correctifs de sécurité pour des systèmes qui ne sont plus supportés (Windows 7 et Windows Server 2008R2).

Le CERT-FR a connaissance de références publiques mettant en exergue des travaux ayant potentiellement débouché sur l'élaboration d'un code d'exploitation pour l'une de ces vulnérabilités, et citant une intention de publication prochaine d'un article. Le CERT-FR recommande fortement d'appliquer les correctifs et, le cas échéant, de mettre en œuvre les moyens d'atténuation proposés par l'éditeur.

Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

Documentation

- Bulletin de sécurité Microsoft CVE-2022-34718 du 13 septembre 2022
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34718
- Bulletin de sécurité Microsoft CVE-2022-34721 du 13 septembre 2022
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34721
- Bulletin de sécurité Microsoft CVE-2022-34722 du 13 septembre 2022
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34722
- Référence CVE CVE-2022-34718
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34718
- Référence CVE CVE-2022-34721
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34721
- Référence CVE CVE-2022-34722
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34722

Gestion détaillée du document

le 16 septembre 2022
Version initiale

Conditions d'utilisation de ce document : https://www.cert.ssi.gouv.fr
Dernière version de ce document : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-007/