Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 août 2017
N° CERTFR-2017-AVI-261

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Microsoft Windows

Gestion du document

Référence	CERTFR-2017-AVI-261
Titre	Multiples vulnérabilités dans Microsoft Windows
Date de la première version	09 août 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft du 08 août 2017 Bulletin de sécurité Microsoft b3d96835-f651-e711-80dd-000d3a32fc99 du 08 août 2017
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

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

1 - Risque(s)

- exécution de code arbitraire à distance
- déni de service à distance
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- Windows 10 Version 1511 pour systèmes 32 bits
- Windows 10 Version 1511 pour systèmes x64
- Windows 10 Version 1607 pour systèmes 32 bits
- Windows 10 Version 1607 pour systèmes x64
- Windows 10 Version 1703 pour systèmes 32 bits
- Windows 10 Version 1703 pour systèmes x64
- Windows 10 pour systèmes 32 bits
- Windows 10 pour systèmes x64
- Windows 7 pour systèmes 32 bits Service Pack 1
- Windows 7 pour systèmes x64 Service Pack 1
- Windows 8.1 pour systèmes 32 bits

- Windows 8.1 pour systèmes x64
- Windows RT 8.1
- Windows Server 2008 R2 pour systèmes Itanium Service Pack 1
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1 (Server Core installation)
- Windows Server 2008 pour systèmes 32 bits Service Pack 2
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 (Server Core installation)
- Windows Server 2008 pour systèmes Itanium Service Pack 2
- Windows Server 2008 pour systèmes x64 Service Pack 2
- Windows Server 2008 pour systèmes x64 Service Pack 2 (Server Core installation)
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Microsoft Windows*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité Microsoft du 08 août 2017
  https://portal.msrc.microsoft.com/fr-fr/security-guidance
- Bulletin de sécurité Microsoft b3d96835-f651-e711-80dd-000d3a32fc99 du 08 août 2017
  https://portal.msrc.microsoft.com/fr-fr/security-guidance/releasenotedetail/b3d96835-f651-e711-80dd-000d3a32fc99
- Référence CVE CVE-2017-0174
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0174
- Référence CVE CVE-2017-0250
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0250
- Référence CVE CVE-2017-0293
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0293
- Référence CVE CVE-2017-8591
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8591
- Référence CVE CVE-2017-8593
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8593
- Référence CVE CVE-2017-8620
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8620
- Référence CVE CVE-2017-8622
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8622
- Référence CVE CVE-2017-8623
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8623
- Référence CVE CVE-2017-8624
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8624

- Référence CVE CVE-2017-8627
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8627
- Référence CVE CVE-2017-8633
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8633
- Référence CVE CVE-2017-8664
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8664
- Référence CVE CVE-2017-8666
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8666
- Référence CVE CVE-2017-8668
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8668
- Référence CVE CVE-2017-8673
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8673
- Référence CVE CVE-2017-8691
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8691

Gestion détaillée du document

09 août 2017 version initiale.