Centre de Veille de Détection et
de Réaction aux Attaques
Informatiques

مركز اليقظة والرصد
والتصدي للهجمات المعلوماتية

# Bulletin de sécurité du maCERT

## Titre: Vulnérabilités affectant plusieurs produits de Microsoft

**Numéro de Référence : 19801303/19**
**Risque : Important**
**Impact : Important**
**Systèmes affectés**

- Microsoft Internet Explorer 9, 10 et 11
- Microsoft Edge
- Microsoft Office 2010 Service Pack 2
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Foundation 2013 Service Pack 1
- Windows 7, 8, 8.1 et 10.
- Windows server 2008, 2012, 2016 et 2018.
- .NET Core SDK versions 1.1 et 2.1.500
- ChakraCore
- Microsoft Dynamics 365 (on-premises) version 8
- Microsoft Lync Server 2013 July 2018 Update
- Microsoft Visual Studio 2017 version 15.9
- Mono Framework Versions 5.18.0.223 et 5.20.0
- Skype pour Business Server 2015 March 2019 Update
- Team Foundation Server 2017 Update 3.1
- Team Foundation Server 2018 Update 3.2
- Team Foundation Server 2018 Updated 1.2

**Identificateurs externes**

CVE-2019-0748, CVE-2019-0778, CVE-2019-0609, CVE-2019-0680, CVE-2019-0746, CVE-2019-0667, CVE-2019-0666, CVE-2019-0665, CVE-2019-0761, CVE-2019-0780, CVE-2019-0762, CVE-2019-0783, CVE-2019-0768, CVE-2019-0763, CVE-2019-0701, CVE-2019-0702, CVE-2019-0703, CVE-2019-0704, CVE-2019-0775, CVE-2019-0603, CVE-2019-0772, CVE-2019-0726, CVE-2019-0690, CVE-2019-0614, CVE-2019-0617 CVE-2019-0766, CVE-2019-0767, CVE-2019-0765, CVE-2019-0756, CVE-2019-0755 CVE-2019-0754, CVE-2019-0797, CVE-2019-0782, CVE-2019-0784, CVE-2019-0759

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

**Bilan de la vulnérabilité**

Plusieurs vulnérabilités ont été corrigées dans certains produits Microsoft. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une élévation de privilèges, divulguer des informations confidentielles, exécuter du code arbitraire à distance ou causer un déni de service.

**Solution**

Veuillez-vous référer au guide de sécurité de Microsoft pour obtenir les nouvelles mises à jour :

- https://portal.msrc.microsoft.com/en-us/security-guidance

**Risque :**

- Exécution de code arbitraire à distance.
- Déni de service.
- Accès à des informations confidentielles.
- Elévation de privilèges.

**Annexe**

Veuillez-vous référer aux guides de sécurité de Microsoft pour obtenir les nouvelles mises à jour :

- https://portal.msrc.microsoft.com/en-us/security-guidance