



BULLETIN DE SECURITE

Titre : Vulnérabilités dans les produits Microsoft

Numéro de Référence : 22040910/19

Risque : Important

Impact : Important

Systemes affectés

- Microsoft Excel 2010 Service Pack 2 (éditions 32 bits)
- Microsoft Excel 2010 Service Pack 2 (éditions 64 bits)
- Microsoft Excel 2013 RT Service Pack 1
- Microsoft Excel 2013 Service Pack 1 (éditions 32 bits)
- Microsoft Excel 2013 Service Pack 1 (éditions 64 bits)
- Microsoft Excel 2016 (édition 32 bits)
- Microsoft Excel 2016 (édition 64 bits)
- Microsoft Office 2010 Service Pack 2 (éditions 32 bits)
- Microsoft Office 2010 Service Pack 2 (éditions 64 bits)
- Microsoft Office 2013 RT Service Pack 1
- Microsoft Office 2013 Service Pack 1 (éditions 32 bits)
- Microsoft Office 2013 Service Pack 1 (éditions 64 bits)
- Microsoft Office 2016 (édition 32 bits)
- Microsoft Office 2016 (édition 64 bits)
- Microsoft Office 2016 pour Mac
- Microsoft Office 2019 pour Mac
- Microsoft Office 2019 pour éditions 32 bits
- Microsoft Office 2019 pour éditions 64 bits
- Microsoft SharePoint Enterprise Server 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Foundation 2010 Service Pack 2

- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft SharePoint Server 2010 Service Pack 2
- Microsoft SharePoint Server 2019
- Office 365 ProPlus pour 64 bits Systems
- Office 365 ProPlus pour systèmes 32 bits
- 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 1703 for 32-bit Systems
- Windows 10 Version 1703 for x64-based Systems
- Windows 10 Version 1709 for 32-bit Systems
- Windows 10 Version 1709 for 64-based Systems
- Windows 10 Version 1709 for ARM64-based Systems
- Windows 10 Version 1803 for 32-bit Systems
- Windows 10 Version 1803 for ARM64-based Systems
- Windows 10 Version 1803 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 1903 for 32-bit Systems
- Windows 10 Version 1903 for ARM64-based Systems
- Windows 10 Version 1903 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 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 Itanium-Based Systems Service Pack 2
- 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 Itanium-Based Systems Service Pack 1
- 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 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server, version 1803 (Server Core Installation)
- Windows Server, version 1903 (Server Core installation)
- Azure DevOps Server 2019
- Azure Linux Guest Agent
- ChakraCore
- Microsoft Exchange Server 2010 Service Pack 3
- Microsoft Exchange Server 2013 Cumulative Update 22
- Microsoft Exchange Server 2016 Cumulative Update 11
- Microsoft Exchange Server 2016 Cumulative Update 12
- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2019 Cumulative Update 1
- Open Enclave SDK
- Team Foundation Server 2015 Update 4.2
- Team Foundation Server 2017 Update 3.1
- Team Foundation Server 2018 Update 3.2
- Team Foundation Server 2018 Updated 1.2
- ASP.NET Core 2.2
- Microsoft Edge
- Internet Explorer 10
- Internet Explorer 11
- Internet Explorer 9

### **Identificateurs externes**

- CVE-2019-1070 , CVE-2019-1230 , CVE-2019-1313 , CVE-2019-1314 , CVE-2019-1327 ,
- CVE-2019-1328 , CVE-2019-1329 , CVE-2019-1330 , CVE-2019-1331 , CVE-2019-1334 ,
- CVE-2019-1337 , CVE-2019-1344 , CVE-2019-1345 , CVE-2019-1358 , CVE-2019-1359 ,
- CVE-2019-1361 , CVE-2019-1363 , CVE-2019-1369 , CVE-2019-1378

## Bilan de la vulnérabilité

Microsoft a publié le patch Tuesday du mois Octobre 2019. Les mises à jour de ce mois-ci corrigent 59 failles parmi eux 9 sont classées comme critique. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une élévation de privilèges, une divulgation d'informations, une exécution de code à distance et un déni de service.

### Solution :

Veillez-vous référer aux bulletins de sécurité Microsoft du 08 Octobre 2019:

- <https://portal.msrc.microsoft.com/fr-FR/security-guidance>

### Risque :

- Divulgation d'informations ;
- Déni de service ;
- Exécution de code à distance ;
- Élévation de privilèges.

### Référence :

Bulletin de sécurité Microsoft du 08 Octobre 2019:

<https://portal.msrc.microsoft.com/fr-FR/security-guidance>