

Alerta de seguridad informática	9VSA20-00122-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de enero de 2020
Última revisión	15 de enero de 2020

## NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft en su reporte mensual de actualizaciones correspondiente a Enero de 2020, parchando 14 vulnerabilidades en sus softwares. Además se informa de 36 vulnerabilidades adicionales al reporte mensual.

Entre la información entregada por Microsoft, se destaca la vulnerabilidad CVE-2020-0601, ya que esta vulnerabilidad afecta a todas las máquinas que ejecutan sistemas operativos Windows 10 de 32 o 64 bits, incluidas las versiones de Windows Server 2016 y 2019. Esta vulnerabilidad permite que la validación del certificado de Elliptic Curve Cryptography (ECC) omita el almacén de confianza, permitiendo que el software no deseado o malicioso se disfrace como firmado auténticamente por una organización confiable. Esto podría engañar a los usuarios o frustrar los métodos de detección de malware, como los antivirus. Además, se podría emitir un certificado creado con fines malintencionados para un nombre de host que no lo autorizó, y un navegador que se base en Windows CryptoAPI no emitiría una advertencia, lo que permitiría a un atacante descifrar, modificar o inyectar datos en las conexiones del usuario sin detección.

## Vulnerabilidades

Reportados en el informe de Enero:

CVE-2020-0601  
CVE-2020-0607  
CVE-2020-0608  
CVE-2020-0615  
CVE-2020-0622  
CVE-2020-0637  
CVE-2020-0639  
CVE-2020-0643  
CVE-2020-0647  
CVE-2020-0650  
CVE-2020-0651  
CVE-2020-0652  
CVE-2020-0653  
CVE-2020-0654

Reportador adicionalmente:

CVE-2019-1491  
CVE-2020-0602  
CVE-2020-0603  
CVE-2020-0605  
CVE-2020-0606  
CVE-2020-0609  
CVE-2020-0610  
CVE-2020-0611  
CVE-2020-0612  
CVE-2020-0613  
CVE-2020-0614  
CVE-2020-0616  
CVE-2020-0617  
CVE-2020-0620  
CVE-2020-0621  
CVE-2020-0623  
CVE-2020-0624  
CVE-2020-0625  
CVE-2020-0626  
CVE-2020-0627  
CVE-2020-0628  
CVE-2020-0629  
CVE-2020-0630  
CVE-2020-0631  
CVE-2020-0632  
CVE-2020-0633

CVE-2020-0634  
CVE-2020-0635  
CVE-2020-0636  
CVE-2020-0638  
CVE-2020-0640  
CVE-2020-0641  
CVE-2020-0642  
CVE-2020-0644  
CVE-2020-0646  
CVE-2020-0656

### Productos Afectados

- .NET Core 3.0 y 3.1
- ASP.NET Core 2.1, 3.0 y 3.1
- Dynamics 365 Field Service (on-premises) v7 series
- Internet Explorer 9, 10, 11
- Microsoft .NET Framework
  - 3.0 Service Pack 2
  - 3.5
  - 4.8 y anteriores
- Microsoft Excel
  - 2010 Service Pack 2 (32-bit y 64-bit editions)
  - 2013 RT Service Pack 1
  - 2013 Service Pack 1 (32-bit y 64-bit editions)
  - 2016 (32-bit y 64-bit editions)
- Microsoft Office
  - 2010 Service Pack 2 (32-bit y 64-bit editions)
  - 2013 RT Service Pack 1
  - 2013 Service Pack 1 (32-bit y 64-bit editions)
  - 2016 (32-bit y 64-bit editions)
  - 2016 for Mac
  - 2019 (32-bit y 64-bit editions)
  - 2019 for Mac
- Microsoft SharePoint
  - Enterprise Server 2016
  - Foundation 2010 Service Pack 2
  - Foundation 2013 Service Pack 1
  - Server 2019
- Office 365 ProPlus (32-bit y 64-bit editions)
- Office Online Server

- One Drive for Android
- Windows 10
  - Version 1607, 1703, 1709, 1803, 1809, 1903, para 32 y 64 bit
- Windows 7
  - 32-bit Systems Service Pack 1
  - x64-based Systems Service Pack 1
- Windows 8.1
  - 32-bit systems
  - x64-based systems
- Windows Defender
- Windows RT 8.1
- Windows Server 2008
  - 32-bit Systems Service Pack 2
  - 32-bit Systems Service Pack 2 (Server Core installation)
  - Itanium-Based Systems Service Pack 2
  - x64-based Systems Service Pack 2
  - x64-based Systems Service Pack 2 (Server Core installation)
  - R2 for Itanium-Based Systems Service Pack 1
  - R2 for x64-based Systems Service Pack 1
  - R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2012
  - 2012
  - Server Core installation
  - R2 y R2 (Server Core installation)
- Windows Server 2016
  - 2016
  - Server Core installation
- Windows Server 2019
  - 2019
  - Server Core installation
- Windows Server
  - version 1803 (Server Core Installation)
  - version 1903 (Server Core installation)

### Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

## Enlace

<https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Jan>  
<https://portal.msrc.microsoft.com/en-us/security-guidance>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0607>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0608>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0615>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0622>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0637>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0639>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0643>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0647>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0650>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0651>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0652>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0653>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0654>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1491>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0602>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0603>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0605>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0606>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0611>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0612>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0613>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0614>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0616>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0617>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0620>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0621>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0623>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0624>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0625>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0626>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0627>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0628>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0629>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0630>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0631>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0632>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0633>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0634>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0635>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0636>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0638>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0640>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0641>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0642>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0644>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0646>  
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0656>