Alerta de seguridad informática	9VSA20-00153-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de marzo de 2020
Última revisión	10 de marzo 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 marzo de 2020, parchando 26 vulnerabilidades en sus softwares, además se informa de 89 vulnerabilidades adicionales al reporte mensual.

Un aviso importante además de las actualizaciones es un reporte (ADV200005) referente al servicio SMBv3 en el cual posee una vulnerabilidad aún no parchada, sin embargo, Microsoft recomienda una solución alterna. En este informe se dará un breve detalle de lo reportado por Microsoft.

Vulnerabilidades

Reportados en el informe de marzo:
CVE-2020-0765
CVE-2020-0774
CVE-2020-0775
CVE-2020-0795
CVE-2020-0813
CVE-2020-0820
CVE-2020-0850
CVE-2020-0851
CVE-2020-0852
CVE-2020-0853
CVE-2020-0855
CVE-2020-0859
CVE-2020-0861
CVE-2020-0863

CVE-2020-0871
CVE-2020-0874
CVE-2020-0876
CVE-2020-0879
CVE-2020-0880
CVE-2020-0882
CVE-2020-0885
CVE-2020-0891
CVE-2020-0892
CVE-2020-0893
CVE-2020-0894
CVE-2020-0902

Reportado adicionalmente:

ADV200005	CVE-2020-0799	CVE-2020-0840
CVE-2020-0645	CVE-2020-0800	CVE-2020-0841
CVE-2020-0684	CVE-2020-0801	CVE-2020-0842
CVE-2020-0690	CVE-2020-0802	CVE-2020-0843
CVE-2020-0700	CVE-2020-0803	CVE-2020-0844
CVE-2020-0758	CVE-2020-0804	CVE-2020-0845
CVE-2020-0762	CVE-2020-0806	CVE-2020-0847
CVE-2020-0763	CVE-2020-0807	CVE-2020-0848
CVE-2020-0768	CVE-2020-0808	CVE-2020-0849
CVE-2020-0769	CVE-2020-0809	CVE-2020-0854
CVE-2020-0770	CVE-2020-0810	CVE-2020-0857
CVE-2020-0771	CVE-2020-0811	CVE-2020-0858
CVE-2020-0772	CVE-2020-0812	CVE-2020-0860
CVE-2020-0773	CVE-2020-0814	CVE-2020-0864
CVE-2020-0776	CVE-2020-0815	CVE-2020-0865
CVE-2020-0777	CVE-2020-0816	CVE-2020-0866
CVE-2020-0778	CVE-2020-0819	CVE-2020-0867
CVE-2020-0779	CVE-2020-0822	CVE-2020-0868
CVE-2020-0780	CVE-2020-0823	CVE-2020-0869
CVE-2020-0781	CVE-2020-0824	CVE-2020-0872
CVE-2020-0783	CVE-2020-0825	CVE-2020-0877
CVE-2020-0785	CVE-2020-0826	CVE-2020-0881
CVE-2020-0786	CVE-2020-0827	CVE-2020-0883
CVE-2020-0787	CVE-2020-0828	CVE-2020-0884
CVE-2020-0788	CVE-2020-0829	CVE-2020-0887
CVE-2020-0789	CVE-2020-0830	CVE-2020-0896
CVE-2020-0791	CVE-2020-0831	CVE-2020-0897
CVE-2020-0793	CVE-2020-0832	CVE-2020-0898
CVE-2020-0797	CVE-2020-0833	CVE-2020-0903
CVE-2020-0798	CVE-2020-0834	CVE-2020-0905

Microsoft es consciente de una vulnerabilidad de ejecución remota de código en la forma en que el protocolo Microsoft Server Message Block 3.1.1 (SMBv3) maneja ciertas solicitudes. Un atacante que aproveche con éxito la vulnerabilidad podría obtener la capacidad de ejecutar código en el servidor SMB o el cliente SMB de destino.

Para aprovechar la vulnerabilidad contra un servidor SMB, un atacante no autenticado podría enviar un paquete especialmente diseñado a un servidor SMBv3 de destino. Para aprovechar la vulnerabilidad contra un cliente SMB, un atacante no autenticado necesitaría configurar un servidor SMBv3 malicioso y convencer a un usuario para que se conecte a él.

Aún no existe un parche para mitigar esta vulnerabilidad, como solución alterna Microsoft recomienda lo siguiente:

Deshabilitar la compresión SMBv3

Puede deshabilitar la compresión para impedir que los atacantes no autenticados aprovechen la vulnerabilidad contra un servidor SMBv3 con el siguiente comando de PowerShell:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
DisableCompression -Type DWORD -Value 1 -Force
```

- No es necesario reiniciar después de realizar el cambio.
- Esta solución alternativa no impide la explotación de clientes SMB.

Puede deshabilitar la solución alternativa con el siguiente comando de PowerShell.

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
DisableCompression -Type DWORD -Value 0 -Force
```

Microsoft recomienda encarecidamente que instale las actualizaciones para esta vulnerabilidad tan pronto como estén disponibles, incluso si planea dejar esta solución alternativa en su lugar.

Productos Afectados

- Application Inspector
- Azure DevOps Server 2019 (Update 1, Update 1.1)
- Azure DevOps Server 2019.0.1
- ChakraCore
- Dynamics 365 Business Central 2019 Release Wave 2 (On-Premise)
- Dynamics 365 Business Central 2019 Spring Update
- Internet Explorer 9, 10, 11
- Microsoft Business Productivity Servers 2010 Service Pack 2
- Microsoft Dynamics 365 BC On Premise

- Microsoft Dynamics NAV
  - 2013
  - 2015
  - 2016
  - 2017
  - 2018
- Microsoft Edge (EdgeHTML-based)
- Microsoft Exchange Server
  - 2016 Cumulative Update 14
  - 2016 Cumulative Update 15
  - 2019 Cumulative Update 3
  - 2019 Cumulative Update 4
- Microsoft Office
  - 2010 (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
  - Online Server
  - Web Apps 2010 Service Pack 2
- Microsoft SharePoint
  - Enterprise Server 2016, 2013 service Pack 1 y Service Pack 2
  - Foundation 2013 Service Pack 1 y 2010 Service Pack 2
  - Server 2019
- Microsoft SQL Server
  - 2012 for 32-bit Systems Service Pack 4 (QFE)
  - 2012 for x64-based Systems Service Pack 4 (QFE)
  - 2014 Service Pack 3 for 32-bit Systems (CU)
  - 2014 Service Pack 3 for 32-bit Systems (GDR)
  - 2014 Service Pack 3 for x64-based Systems (CU)
  - 2014 Service Pack 3 for x64-based Systems (GDR)
  - 2016 for x64-based Systems Service Pack 2 (CU)
  - 2016 for x64-based Systems Service Pack 2 (GDR)
- Office 365 ProPlus (32-bit y 64-bit editions)
- Windows 10
  - Version 1607, 1709, 1803, 1809, 1903, 1909, 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 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)
  - version 1909 (Server Core installation)

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200005
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0645
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0684
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0690
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0700
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0758
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0762
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0763
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0765
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0768
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0769
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0770
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0771
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0772
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0773
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0774

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0775
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0776
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0777
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0778
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0779
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0780
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0781
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0783
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0785
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0786
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0787
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0788
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0789
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0791
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0793
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0795
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0797
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0798
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0799
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0800
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0801
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0802
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0803
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0804
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0806
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0807
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0808
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0809
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0810
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0811
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0812
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0813
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0814
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0815
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0816
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0819
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0820
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0822
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0823
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0824
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0825
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0826
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0827
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0828
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0829
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0830

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0831
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0832
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0833
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0834
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0840
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0841
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0842
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0843
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0844
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0845
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0847
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0848
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0849
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0850
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0851
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0852
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0853
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0854
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0855
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0857
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0858
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0859
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0860
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0861
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0863
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0864
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0865
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0866
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0867
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0868
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0869
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0871
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0872
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0874
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0876
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0877
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0879
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0880
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0881
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0882
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0883
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0884
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0885
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0887
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0891
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0892

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0893
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0894
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0896
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0897
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0898
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0902
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0903
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0905

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.13 15:48:40 -03'00'