Alerta de seguridad cibernética	9VSA20-00302-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de octubre de 2020
Última revisión	14 de octubre 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 octubre de 2020, parchando 28 vulnerabilidades en sus softwares clasificando a dos de ellas como crítica y 26 como importantes, además se informa de 60 vulnerabilidades adicionales al reporte mensual, 10 de ellas clasificadas como críticas y 50 como importantes.

Vulnerabilidades

Informadas en el reporte mensual correspondiente al mes de julio

ADV200012	CVE-2020-16928	CVE-2020-16942
CVE-2020-16889	CVE-2020-16929	CVE-2020-16947
CVE-2020-16896	CVE-2020-16930	CVE-2020-16949
CVE-2020-16897	CVE-2020-16931	CVE-2020-16954
CVE-2020-16901	CVE-2020-16932	CVE-2020-16955
CVE-2020-16904	CVE-2020-16933	CVE-2020-16957
CVE-2020-16914	CVE-2020-16934	CVE-2020-16969
CVE-2020-16918	CVE-2020-16937	CVE-2020-16995
CVE-2020-16919	CVE-2020-16938	
CVE-2020-16921	CVE-2020-16941	

Vulnerabilidades adicionales informadas

CVE-2020-0764	CVE-2020-16905	CVE-2020-16944
CVE-2020-1047	CVE-2020-16907	CVE-2020-16945
CVE-2020-1080	CVE-2020-16908	CVE-2020-16946
CVE-2020-1167	CVE-2020-16909	CVE-2020-16948
CVE-2020-1243	CVE-2020-16910	CVE-2020-16950
CVE-2020-16863	CVE-2020-16911	CVE-2020-16951
CVE-2020-16876	CVE-2020-16912	CVE-2020-16952
CVE-2020-16877	CVE-2020-16913	CVE-2020-16953
CVE-2020-16885	CVE-2020-16915	CVE-2020-16956
CVE-2020-16886	CVE-2020-16916	CVE-2020-16967
CVE-2020-16887	CVE-2020-16920	CVE-2020-16968
CVE-2020-16890	CVE-2020-16922	CVE-2020-16972
CVE-2020-16891	CVE-2020-16923	CVE-2020-16973
CVE-2020-16892	CVE-2020-16924	CVE-2020-16974
CVE-2020-16894	CVE-2020-16927	CVE-2020-16975
CVE-2020-16895	CVE-2020-16935	CVE-2020-16976
CVE-2020-16898	CVE-2020-16936	CVE-2020-16977
CVE-2020-16899	CVE-2020-16939	CVE-2020-16978
CVE-2020-16900	CVE-2020-16940	CVE-2020-16980
CVE-2020-16902	CVE-2020-16943	CVE-2020-17003

Impacto

Dependiendo de la vulnerabilidad informada por Microsoft se pueden provocar denegaciones de servicio, elevación de privilegios, acceso a información confidencial, ejecución de código remoto o spoofing. El detalle de cada una de ellas se podrá revisar en los enlaces.

De las vulnerabilidades publicadas hacemos incapié en el CVE-2020-16898 clasificado como crítico, debido a que existe una vulnerabilidad de ejecución remota de código cuando la pila TCP/IP de Windows maneja incorrectamente los paquetes de anuncios de enrutador ICMPv6. Un atacante que aproveche con éxito esta vulnerabilidad podría obtener la capacidad de ejecutar código en el servidor o cliente de destino.

Para aprovechar esta vulnerabilidad, un atacante tendría que enviar paquetes de anuncios de enrutador ICMPv6 especialmente diseñados a una computadora remota con Windows.

La actualización corrige la vulnerabilidad al corregir la forma en que la pila TCP / IP de Windows maneja los paquetes de anuncios de enrutador ICMPv6.

Productos Afectados

- 3D Viewer
- Adobe Flash Player
- Azure Functions
- Dynamics 365 Commerce
- Microsoft .NET Framework
  - 2.0 Service Pack 2
  - 3.5
  - 3.5 y 4.6.2/4.7/4.7.1/4.7.2
  - 3.5 y 4.6/4.6.1/4.6.2
  - 3.5 y 4.7.1/4.7.2
  - 3.5 y 4.7.2
  - 3.5 y 4.8
  - 3.5.1
  - 4.5.2
  - 4.6
  - 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2
  - 4.8
- Microsoft 365 Apps for Enterprise (32-bit y 64-bit)
- Microsoft Dynamics 365 (on-premises) version 8.2 y 9.0
- Microsoft Excel
  - 2010 Service Pack 2 (32-bit y 64-bit)
  - 2013 RT Service Pack 1
  - 2013 Service Pack 2 (32-bit y 64-bit)
  - 2016 (32-bit y 64-bit)
- Microsoft Excel Web App 2010 Service Pack 2
- Microsoft Exchange Server
  - 2013 Cumulative Update 23
  - 2016 Cumulative Update 17
  - 2016 Cumulative Update 18
  - 2019 Cumulative Update 6
  - 2019 Cumulative Update 7
- Microsoft Office
  - 2010 Service Pack 2 (32-bit y 64-bit editions)
  - 2013 Click-to-Run (C2R) (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
  - Online Server
  - Web Apps 2013 Service Pack 1
  - Web Apps 2010 Service Pack 2
- Microsoft Outlook
  - 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 SharePoint
  - Enterprise Server 2013 Service Pack 1
  - Enterprise Server 2016
  - Foundation 2010 Service Pack 2
  - Foundation 2013 Service Pack 1
  - Server 2010 Service Pack 2
  - Server 2019
- Microsoft Word
  - 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)
- Network Watcher Agent virtual machine extension for Linux
- PowerShellGet 2.2.5
- Visual Studio Code
- Windows 10 (32-bit y 64-bit)
  - Version 1607, 1709, 1803, 1809, 1903, 1909, 2004, para 32 bit, 64 bit y ARM64-based
- 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)
- x64-based Systems Service Pack 2
- x64-based Systems Service Pack 2 (Server Core installation)
- 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 1903 (Server Core installation)
  - version 1909 (Server Core installation)
  - version 2004 (Server Core installation)

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlaces

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Oct
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200012
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16889
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16896
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16897
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16901
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16904
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16914
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16918
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16919
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16921
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16928
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16929
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16930
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16931
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16932
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16933
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16934
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16937
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16938
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16941
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16942
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16947
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16949
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16954
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16955
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16957
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16969
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16995
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0764
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1047
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1080
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1167
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1243
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16863
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16876
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16877
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16885

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16886
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16887
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16890
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16891
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16892
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16894
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16895
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16899
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16900
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16902
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16905
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16907
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16908
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16909
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16910
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16911
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16912
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16913
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16915
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16916
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16920
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16922
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16923
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16924
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16927
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16935
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16936
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16939
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16940
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16943
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16944
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16945
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16946
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16948
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16950
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16951
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16952
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16953
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16956
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16967
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16968
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16972
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16973
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16974

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16975
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16976
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16977
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16978
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16980
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17003