Alerta de seguridad cibernética	9VSA22-00632-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2022
Última revisión	10 de mayo de 2022

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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno, comparte la información que comparte mensualmente Microsoft sobre nuevas vulnerabilidades en sus productos, parte de su tradicional “Update Tuesday”.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2022-21972
CVE-2022-21978
CVE-2022-22011
CVE-2022-22012
CVE-2022-22013
CVE-2022-22014
CVE-2022-22015
CVE-2022-22016
CVE-2022-22017
CVE-2022-22019
CVE-2022-22713
CVE-2022-23267
CVE-2022-23270
CVE-2022-23279
CVE-2022-24466
CVE-2022-26913
CVE-2022-26923
CVE-2022-26925
CVE-2022-26926
CVE-2022-26927
CVE-2022-26930
CVE-2022-26931
CVE-2022-26932
CVE-2022-26933
CVE-2022-26934
CVE-2022-26935
CVE-2022-26936
CVE-2022-26937
CVE-2022-26938
CVE-2022-26939
CVE-2022-26940
CVE-2022-29102
CVE-2022-29103
CVE-2022-29104
CVE-2022-29105
CVE-2022-29106
CVE-2022-29107
CVE-2022-29108
CVE-2022-29109
CVE-2022-29110
CVE-2022-29112
CVE-2022-29113
CVE-2022-29114
CVE-2022-29115
CVE-2022-29116
CVE-2022-29117
CVE-2022-29120
CVE-2022-29121
CVE-2022-29122
CVE-2022-29123
CVE-2022-29125
CVE-2022-29126
CVE-2022-29127
CVE-2022-29128
CVE-2022-29129
CVE-2022-29130
CVE-2022-29131
CVE-2022-29132
CVE-2022-29133
CVE-2022-29134
CVE-2022-29135
CVE-2022-29137
CVE-2022-29138
CVE-2022-29139
CVE-2022-29140
CVE-2022-29141
CVE-2022-29142
CVE-2022-29145
CVE-2022-29148
CVE-2022-29150
CVE-2022-29151
CVE-2022-30129
CVE-2022-30130

Impacto

Vulnerabilidades de día cero actualmente explotadas

CVE-2022-26925: Vulnerabilidad de spoofing en Windows LSA.

CVE-2022-29972: Vulnerabilidad en Magnitude Simba Amazon Redshift ODBC Driver (conocida como "SynLapse").

CVE-2022-22713: Vulnerabilidad de denegación de servicio en Windows Hyper-V.

Vulnerabilidades críticas

CVE-2022-21972: Vulnerabilidad de ejecución remota de código en Point-to-Point Tunneling Protocol de Windows. El atacante no requiere permisos ni privilegios.

CVE-2022-22017: Vulnerabilidad de ejecución remota de código en Remote Desktop Client de Windows. El atacante no requiere permisos ni privilegios.

CVE-2022-23270: Vulnerabilidad de ejecución remota de código en Point-to-Point Tunneling Protocol de Windows. El atacante no requiere permisos ni privilegios.

CVE-2022-26923: Vulnerabilidad de elevación de privilegios en Active Directory Domain Services de Windows. El atacante requiere privilegios de nivel de usuario básico para realizar este ataque.

CVE-2022-26931: Vulnerabilidad de elevación de privilegios en Kerberos. El atacante requiere privilegios de nivel de usuario básico para realizar este ataque.

CVE-2022-26937: Vulnerabilidad de ejecución remota de código en Windows Network File System. El atacante no requiere permisos ni privilegios.

Productos afectados

.NET 5.0
.NET 6.0
.NET Core 3.1
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.8

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Exchange Server 2013 Cumulative Update 23
Microsoft Exchange Server 2016 Cumulative Update 22
Microsoft Exchange Server 2016 Cumulative Update 23
Microsoft Exchange Server 2019 Cumulative Update 11
Microsoft Exchange Server 2019 Cumulative Update 12
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Publisher 2013 Service Pack 1 (32-bit editions)
Microsoft Publisher 2013 Service Pack 1 (64-bit editions)
Microsoft Publisher 2016 (32-bit edition)
Microsoft Publisher 2016 (64-bit edition)
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Microsoft Visual Studio 2022 version 17.0
Microsoft Visual Studio 2022 version 17.1
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Remote Desktop client for Windows Desktop
Visual Studio Code
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 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems

Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 11 for ARM64-based Systems
Windows 11 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 RT 8.1
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 x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
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 2022
Windows Server 2022 (Server Core installation)
Windows Server, version 20H2 (Server Core Installation)

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://msrc.microsoft.com/update-guide/releaseNote/2022-May
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21972
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21978
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22011

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22713
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23267
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23270
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23279
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24466
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26913
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26923
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26925
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26926
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26927
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26930
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26931
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26932
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26933
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26934
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26935
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26936
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26937
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26938
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26939
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26939
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29102
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29103
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29104
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29105
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29106
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29107
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29108
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29109
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29110
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29112
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29113
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29114
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29115
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29116
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29117
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29120
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29121

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29122
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29123
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29125
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29126
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29127
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29128
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29129
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29130
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29131
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29132
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29133
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29134
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29135
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29137
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29138
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29139
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29140
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29141
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29142
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29145
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29148
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29150
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29151
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30129
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30130