Alerta de seguridad cibernética	9VSA22-0068X-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2022
Última revisión	9 de agosto 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 Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre vulnerabilidades que afectan a algunos productos de Microsoft, difundidos por la empresa como parte de su actualización mensual "Update Tuesday" correspondiente a agosto.

Vulnerabilidades

CVE-2022-35794	CVE-2022-35765	CVE-2022-35783	CVE-2022-35824
CVE-2022-35766	CVE-2022-35764	CVE-2022-35809	CVE-2022-35757
CVE-2022-35804	CVE-2022-35760	CVE-2022-35782	CVE-2022-35827
CVE-2022-35767	CVE-2022-35754	CVE-2022-35808	CVE-2022-34303
CVE-2022-35753	CVE-2022-35795	CVE-2022-35807	CVE-2022-34692
CVE-2022-35752	CVE-2022-35772	CVE-2022-35781	CVE-2022-35762
CVE-2022-35745	CVE-2022-35797	CVE-2022-35780	CVE-2022-35821
CVE-2022-35744	CVE-2022-35763	CVE-2022-35777	CVE-2022-35788
CVE-2022-34714	CVE-2022-35820	CVE-2022-34703	CVE-2022-35813
CVE-2022-34702	CVE-2022-35779	CVE-2022-33670	CVE-2022-35787
CVE-2022-34696	CVE-2022-35806	CVE-2022-35793	CVE-2022-35786
CVE-2022-34691	CVE-2022-35819	CVE-2022-35802	CVE-2022-35812
CVE-2022-33646	CVE-2022-35818	CVE-2022-35776	CVE-2022-35785
CVE-2022-30133	CVE-2022-35791	CVE-2022-35801	CVE-2022-35811
CVE-2022-24477	CVE-2022-35817	CVE-2022-35775	CVE-2022-35810
CVE-2022-24516	CVE-2022-35816	CVE-2022-35800	CVE-2022-35773
CVE-2022-21980	CVE-2022-35790	CVE-2022-35774	CVE-2022-34686
CVE-2022-35771	CVE-2022-35815	CVE-2022-35799	CVE-2022-30176
CVE-2022-34717	CVE-2022-35789	CVE-2022-35769	CVE-2022-30175
CVE-2022-35768	CVE-2022-35814	CVE-2022-35826	CVE-2022-34685
CVE-2022-35792	CVE-2022-35784	CVE-2022-35825	CVE-2022-35761

CVE-2022-35759	CVE-2022-35743	CVE-2022-34706	CVE-2022-34302
CVE-2022-35758	CVE-2022-35742	CVE-2022-34705	CVE-2022-30194
CVE-2022-35756	CVE-2022-34716	CVE-2022-34704	CVE-2022-30144
CVE-2022-35755	CVE-2022-34715	CVE-2022-34701	CVE-2022-30134
CVE-2022-35751	CVE-2022-34713	CVE-2022-33640	CVE-2022-21979
CVE-2022-35750	CVE-2022-34712	CVE-2022-34699	CVE-2022-30197
CVE-2022-35749	CVE-2022-34710	CVE-2022-34690	CVE-2022-34301
CVE-2022-35748	CVE-2022-34709	CVE-2022-34687	
CVE-2022-35747	CVE-2022-34708	CVE-2022-33648	
CVE-2022-35746	CVE-2022-34707	CVE-2022-33631	

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-21980: Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server.
CVE-2022-24477: Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server.
CVE-2022-24516: Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server.
CVE-2022-30133: Vuln. de ejecución remota de código en Windows Point-to-Point Protocol (PPP).
CVE-2022-33646: Vulnerabilidad de elevación de privilegios en Azure Batch.
CVE-2022-34691: Vulnerabilidad de elevación de privilegios en Active Directory Domain Services.
CVE-2022-34696: Vulnerabilidad de ejecución remota de código en Windows Hyper-V.
CVE-2022-34702: Vulnerabilidad
CVE-2022-34714: Vulnerabilidad de ejecución remota de código en Windows Secure Socket Tunneling Protocol (SSTP).
CVE-2022-35744: Vuln. de ejecución remota de código Windows Point-to-Point Protocol (PPP).
CVE-2022-35745: Vulnerabilidad de ejecución remota de código en Windows Secure Socket Tunneling Protocol (SSTP).
CVE-2022-35752: Vulnerabilidad de ejecución remota de código en Windows Secure Socket Tunneling Protocol (SSTP).
CVE-2022-35753: Vulnerabilidad de ejecución remota de código en Windows Secure Socket Tunneling Protocol (SSTP).
CVE-2022-35766: Vulnerabilidad de ejecución remota de código en Windows Secure Socket Tunneling Protocol (SSTP).
CVE-2022-35767: Vulnerabilidad de ejecución remota de código en Windows Secure Socket Tunneling Protocol (SSTP).
CVE-2022-35794: Vulnerabilidad de ejecución remota de código en Windows Secure Socket Tunneling Protocol (SSTP).
CVE-2022-35804: Vulnerabilidad de ejecución remota de código en SMB Client and Server.

Productos afectados

Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 11 for ARM64-based Systems

Windows 11 for x64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows Server 2022 (Server Core installation)
Windows Server 2022
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 Server 2019 (Server Core installation)
Windows Server 2019
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 7 for x64-based Systems Service Pack 1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server 2016 (Server Core installation)
Windows Server 2016
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for x64-based Systems
Windows RT 8.1
Windows 8.1 for x64-based systems
Windows 8.1 for 32-bit systems
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Azure Batch
Microsoft Exchange Server 2016 Cumulative Update 23
Microsoft Exchange Server 2019 Cumulative Update 12
Microsoft Exchange Server 2019 Cumulative Update 11
Microsoft Exchange Server 2016 Cumulative Update 22
Microsoft Exchange Server 2013 Cumulative Update 23
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1

Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for 32-bit editions
Azure Site Recovery VMWare to Azure
Azure Real Time Operating System GUIX Studio
Microsoft Visual Studio 2015 Update 3
Microsoft Visual Studio 2013 Update 5
Microsoft Visual Studio 2012 Update 5
Microsoft Visual Studio 2022 version 17.0
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 2017 version 15.9 (includes 15.0 - 15.8)
Microsoft Visual Studio 2022 version 17.2
Azure Sphere
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2016 (64-bit edition)
Microsoft Outlook 2016 (32-bit edition)
.NET Core 3.1
.NET 6.0
System Center Operations Manager (SCOM) 2022
System Center Operations Manager (SCOM) 2016
System Center Operations Manager (SCOM) 2019
Microsoft Office Online Server
Open Management Infrastructure
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2016 (64-bit edition)
Microsoft Excel 2016 (32-bit edition)

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35794
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35766
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35804

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35767
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35753
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35752
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35745
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35744
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34714
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34702
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34696
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34691
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33646
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30133
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24477
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24516
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35771
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34717
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35768
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35792
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35765
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35764
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35754
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35795
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35772
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35763
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35820
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35779
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35806
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35819
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35818
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35791
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35817
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35816
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35790
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35815
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35789
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35814
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35784
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35783
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35809
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35782
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35808
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35807
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35781

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35780
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35777
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34703
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33670
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35793
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35802
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35776
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35801
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35775
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35800
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35774
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35799
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35769
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35826
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35757
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34303
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34692
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35762
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35821
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35788
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35813
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35787
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35786
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35812
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35785
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35811
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35810
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35773
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34686
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30176
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30175
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34685
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35761
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35758
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35756
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35755
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35748
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35747

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35746
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35743
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34716
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34715
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34713
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34712
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34710
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34709
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34708
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34707
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34706
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34705
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34704
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34701
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33640
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34699
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34690
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34687
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33648
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33631
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34302
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30194
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30144
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30134
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21979
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30197
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34301

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.08.09 17:13:03 -04'00'