Alerta de seguridad cibernética	9VSA22-00740-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	08 de noviembre de 2022
Última revisión	08 de noviembre 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 entregada por Microsoft sobre las vulnerabilidades parchadas por la empresa como parte de su Update Tuesday mensual, correspondiente a noviembre de 2022.

También el 8 de noviembre, pero separadamente del Update Tuesday, han sido entregados los parches para dos vulnerabilidades, CVE-2022-41040 y CVE-2022-41082, apodadas ProxyNotShell, que han sido previamente alertadas por el CSIRT de Gobierno, quienes también hemos compartido sus medidas de mitigación (alertas www.csirt.gob.cl/noticias/10cnd22-00084-01/ a www.csirt.gob.cl/noticias/10cnd22-00084-05/)

Vulnerabilidades

CVE-2022-23824	CVE-2022-41050	CVE-2022-41078	CVE-2022-41100
CVE-2022-37966	CVE-2022-41051	CVE-2022-41079	CVE-2022-41101
CVE-2022-37967	CVE-2022-41052	CVE-2022-41080	CVE-2022-41102
CVE-2022-37992	CVE-2022-41053	CVE-2022-41082	CVE-2022-41103
CVE-2022-38014	CVE-2022-41054	CVE-2022-41085	CVE-2022-41104
CVE-2022-38015	CVE-2022-41055	CVE-2022-41086	CVE-2022-41105
CVE-2022-38023	CVE-2022-41056	CVE-2022-41088	CVE-2022-41106
CVE-2022-39253	CVE-2022-41057	CVE-2022-41090	CVE-2022-41107
CVE-2022-39327	CVE-2022-41058	CVE-2022-41091	CVE-2022-41109
CVE-2022-41039	CVE-2022-41060	CVE-2022-41092	CVE-2022-41113
CVE-2022-41040	CVE-2022-41061	CVE-2022-41093	CVE-2022-41114
CVE-2022-41044	CVE-2022-41062	CVE-2022-41095	CVE-2022-41116
CVE-2022-41045	CVE-2022-41063	CVE-2022-41096	CVE-2022-41118
CVE-2022-41047	CVE-2022-41064	CVE-2022-41097	CVE-2022-41119
CVE-2022-41048	CVE-2022-41066	CVE-2022-41098	CVE-2022-41120
CVE-2022-41049	CVE-2022-41073	CVE-2022-41099	CVE-2022-41122

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob

CVE-2022-41123 CVE-2022-41125 CVE-2022-41128

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-37966: Vulnerabilidad de elevación de privilegios en Windows Kerberos RC4-HMAC.
CVE-2022-37967: Vulnerabilidad de elevación de privilegios en Windows Kerberos
CVE-2022-38015: Vulnerabilidad de denegación de servicio en Windows Hyper-V.
CVE-2022-39327: Control inapropiado de generación de código ("inyección de código") en Azure CLI.
CVE-2022-41039: Vulnerabilidad de ejecución remota de código en Windows Point-to-Point Tunneling Protocol.
CVE-2022-41044: Vulnerabilidad de ejecución remota de código en Windows Point-to-Point Tunneling Protocol.
CVE-2022-41080: Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server.
CVE-2022-41088: Vulnerabilidad de ejecución remota de código en Windows Point-to-Point Tunneling Protocol.
CVE-2022-41118: Vulnerabilidad de ejecución remota de código en Windows Scripting Languages.

Vulnerabilidades conocidas como "ProxyNotShell":

CVE-2022-41040: Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server.
CVE-2022-41082: Vulnerabilidad de ejecución remota de código en Microsoft Exchange Server.

Productos afectados

Azure CLI
Azure CycleCloud 7
Azure CycleCloud 8
Azure EFLOW
Azure RTOS GUIX Studio
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.7.2
Microsoft .NET Framework 4.8
Microsoft .NET Framework 4.8.1
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 Business Central 2022 Release Wave 1
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 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
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 2022 version 17.0
Microsoft Visual Studio 2022 version 17.2
Microsoft Visual Studio 2022 version 17.3
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)
Nuget 2.1.2
Nuget 4.8.5
SharePoint Server Subscription Edition Language Pack
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 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 10 Version 22H2 for 32-bit Systems
Windows 10 Version 22H2 for ARM64-based Systems
Windows 10 Version 22H2 for x64-based Systems
Windows 11 for ARM64-based Systems
Windows 11 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 Version 22H2 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 2022 Datacenter: Azure Edition (Hotpatch)
Windows Subsystem for Linux (WSL2)
Windows Sysmon

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://msrc.microsoft.com/update-guide/releaseNote/2022-Nov
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37967
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37992
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38015

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39253
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39327
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41039
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41044
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41045
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41047
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41048
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41049
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41050
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41051
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41052
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41053
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41054
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41055
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41056
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41057
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41058
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41060
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41061
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41062
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41063
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41064
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41066
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41073
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41073
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41079
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41080
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41085
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41086
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41088
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41090
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41091
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41092
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41093
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41095
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41096
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41097
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41098
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41099
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41100
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41101
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41102
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41103
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41104
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41105

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41106
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41107
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41109
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41113
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41114
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41116
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41118
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41119
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41120
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41122
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41123
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41125
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41128

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.11.08 18:34:26 -03'00'