



Resource Health Summary

August 14, 2022 05:44 PM clai@sopro.cl

Confidencial: El siguiente informe contiene información confidencial. No lo distribuya, envíe por correo electrónico, envíe por fax o transfiera a través de ningún mecanismo electrónico a menos que haya sido aprobado por la política de seguridad de la empresa receptora. Todas las copias y copias de seguridad de este documento deben guardarse en un almacenamiento protegido en todo momento. No comparta nada de la información contenida en este informe con nadie a menos que estén autorizados para ver la información. La infracción de cualquiera de las instrucciones anteriores es motivo de rescisión.

Nombre del equipo	:	JMATHEUSW10
Sistema operativo	:	Windows 11 Professional Edition (x64)
Paquete de servicio	:	Windows 11 Version 21H2 (x64)
Idioma	:	Español
Estado Correcto	:	Altamente vulnerable
Hora del último parche	:	--
Estado de último análisis	:	Análisis finalizado
Dirección IP	:	192.168.35.17
Dominio	:	CLAIPAYMENTS
Oficina remota	:	Local Office
Usuarios conectados	:	JMATHEUS
Último análisis correcto	:	jul 13, 2022 12:55 PM
Hora del último inicio	:	jul 9, 2022 06:58 PM

Es necesario reiniciar	:	No
------------------------	---	----

Table of Contents

Acerca de

Visión general del estado de los recursos

Vulnerabilidades	2
Errores de configuración del sistema	2
Error de configuración del servidor web	3
Parches	3

Vulnerabilidades a nivel de recursos

Vulnerabilidades de aplicación	4
Vulnerabilidades de servidores web	5
Vulnerabilidades de servidores de bases de datos	5
Sistemas de administración de contenido	5
Vulnerabilidades del día cero	5
Entre iguales	6
Uso compartido del escritorio remoto	6
Final de la vida	6
Excluded Vulnerabilities	6
Excluded Server Vulnerabilities	6
Excluded Risky Software	7

Parches a nivel de recursos

Parches que faltan	8
Parches instalados	9

Parches rechazados	10
Configuraciones de seguridad a nivel de recursos	
Errores de configuración del sistema	11
Error de configuración del servidor web	14
Excluded Misconfiguration	14
Excluded Hardening	14

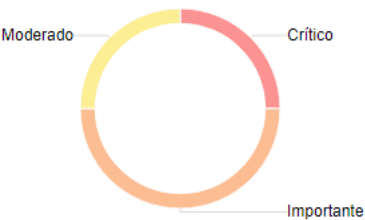
Acerca de

Proporciona una visión general de los parches y vulnerabilidades de un recurso.

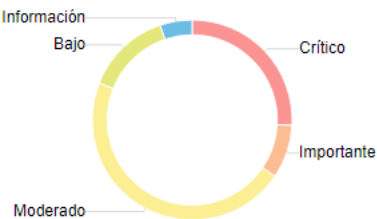
Este informe le ayuda a aliviar la tensión al proporcionarle la lista de parches, sistemas, vulnerabilidades, errores de configuración y otras amenazas sobre los que debe actuar de inmediato. El resumen de estado de los parches le ha proporcionado una vista de nivel superior de los parches que faltan y que están instalados en la red. De prioridad a los parches que faltan utilizando el gráfico de división de gravedad. El siguiente conjunto de secciones le ayuda a comprender el estado del recurso.

Visión general del estado de los recursos

Vulnerabilidades



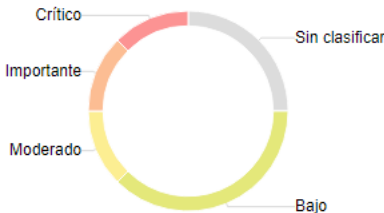
Errores de configuración del sistema



Error de configuración del servidor web

No hay datos disponibles

Parches



Vulnerabilidades a nivel de recursos

Vulnerabilidades de aplicación

Vulnerabilidades	Estado de la vulnerabilidad de seguridad	Disponibilidad de parches	Puntuación de CVSS 3.0	Puntuación de CVSS 2.0	Fecha de publicación	Fecha de actualización	Fecha compatible	Plataforma de sistema operativo
! Multiple vulnerabilities affected in PuTTY (x64) 0.71	✖ No disponible	Disponible	9.8	7.5	ago 18, 2020	ago 18, 2020	ago 18, 2020	Windows
! Windows Container Manager Service Elevation of Privilege Vulnerability for Windows 11 for x64-based Systems (KB5014697)	✖ No disponible	Disponible	10.0	--	jun 14, 2022	jun 14, 2022	jun 14, 2022	Windows
! 19 year old Security Vulnerability in Winrar (x64)	✖ No disponible	Disponible	8.0	7.0	feb 22, 2019	feb 22, 2019	feb 22, 2019	Windows
! Vulnerabilities CVE-2021-33500 are affected in PuTTY (x64) 0.74(x64)	✖ No disponible	Disponible	7.5	5.0	jun 3, 2021	jun 3, 2021	jun 3, 2021	Windows
! Vulnerabilities CVE-2021-36367 are affected in PuTTY 0.75(x64)	✖ No disponible	No disponible	8.0	5.8	jul 16, 2021	jul 16, 2021	jul 16, 2021	Windows
! Vulnerabilities CVE-2021-1811,CVE-2021-1825,CVE-2021-1857 are affected in iCloud 12.0-windows	✖ No disponible	No disponible	7.8	5.8	sep 18, 2021	sep 18, 2021	sep 18, 2021	Windows
Multiple vulnerabilities affected in PuTTY (x64) 0.73	✖ No disponible	Disponible	5.8	4.3	ago 18, 2020	ago 18, 2020	ago 18, 2020	Windows
Vulnerabilities CVE-2020-9952 are fixed in iCloud 11.4	✖ No disponible	No disponible	6.9	5.8	sep 25, 2020	sep 25, 2020	sep 25, 2020	Windows

Vulnerabilidades de servidores web

Vulnerabilidades	Ruta del archivo	Estado de la vulnerabilidad de seguridad	Disponibilidad de parches	Puntuación de CVSS 3.0	Puntuación de CVSS 2.0	Fecha de publicación	Fecha de actualización	Fecha compatible
No se han detectado vulnerabilidades en los criterios especificados								

Vulnerabilidades de servidores de bases de datos

Vulnerabilidades	Ruta del archivo	Estado de la vulnerabilidad de seguridad	Disponibilidad de parches	Puntuación de CVSS 3.0	Puntuación de CVSS 2.0	Fecha de publicación	Fecha de actualización	Fecha compatible
No se han detectado vulnerabilidades en los criterios especificados								

Sistemas de administración de contenido

Vulnerabilidades	Ruta del archivo	Estado de la vulnerabilidad de seguridad	Disponibilidad de parches	Puntuación de CVSS 3.0	Puntuación de CVSS 2.0	Fecha de publicación	Fecha de actualización	Fecha compatible
No se han detectado vulnerabilidades en los criterios especificados								

Vulnerabilidades del día cero

Amenazas	Categoría de amenaza	Tipo de amenaza
Windows Container Manager Service Elevation of Privilege Vulnerability for Windows 11 for x64-based Systems (KB5014697)	CVE-2022-30190	Vulnerabilidad

Entre iguales

Nombre del software	Proveedor
No se ha encontrado software entre iguales con los criterios especificados	

Uso compartido del escritorio remoto

Nombre del software	Proveedor
No se ha encontrado software de escritorio remoto con los criterios especificados	

Final de la vida

Nombre del software	Proveedor	Fecha de vencimiento	Días para que caduque
No se ha encontrado software de final de vida con los criterios especificados			

Excluded Vulnerabilities

Vulnerabilidades	Estado de la vulnerabilidad de seguridad	Disponibilidad de parches	Reason for exclusion	Puntuación de CVSS 3.0	Puntuación de CVSS 2.0	Fecha de publicación	Fecha de actualización	Fecha compatible
No Vulnerabilities are excluded								

Excluded Server Vulnerabilities

Vulnerabilidades	Estado de la vulnerabilidad de seguridad	Disponibilidad de parches	Reason for exclusion	Puntuación de CVSS 3.0	Puntuación de CVSS 2.0	Fecha de publicación	Fecha de actualización	Fecha compatible
No Vulnerabilities are excluded								

Excluded Risky Software

Nombre del software	Proveedor	Reason for exclusion
No Applications are excluded		

Parches a nivel de recursos

Parches que faltan

ID del parche	ID de boletín	Descripción del parche	Proveedor	Tipo de parche	Aprobar estado	Comentarios	Hora de implementación	Desinstalación del parche
 33891	MS22-JUN3	2022-06 Cumulative Update for Windows 11 for x64-based Systems (KB5014697) (CVE-2022-30190)	Microsoft	Security Updates	Aprobado		--	Con asistencia
 109749	MSWU-3506	2022-06 Cumulative Update Preview for Windows 11 for x64-based Systems (KB5014668)	Microsoft	Optional Updates	Aprobado		--	Con asistencia
 109759	MSWU-3507	Update for Microsoft WebView2 Runtime (x64) (103.0.1264.44)	Microsoft	Non Security Updates	Aprobado		--	Sin soporte
 309432	TU-077	Greenshot (1.2.10.6)	Greenshot	Third Party Updates	Aprobado		--	Con asistencia
 322405	TU-855	AirSquirrels Reflector (x64) (4.0.3)	Squirrels	Third Party Updates	Aprobado		--	Con asistencia
 325084	TU-296	PuTTY (x64) (0.77)	Simon Tatham	Third Party Updates	Aprobado		--	Con asistencia
325514	TU-065	Citrix Workspace (22.6.0.60)	Citrix Systems, Inc.	Third Party Updates	Aprobado		--	Sin soporte
 1312245	DU-003	Ethernet Connection (4) [PCI\VEN_8086&DEV_15D8] (12.19.1.37)	Intel	Driver	Aprobado		--	Con asistencia
 1312824	DU-003	Wireless 8265 / 8275 [PCI\VEN_8086&DEV_24FD] (22.110.0.2)	Intel	Driver	Aprobado		--	Con asistencia

Parches instalados

ID del parche	ID de boletín	Descripción del parche	Proveedor	Tipo de parche	Aprobar estado	Comentarios	Hora de implementación	Desinstalación del parche
 10044	MS11-025	Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package MFC Security Update(KB2538242)	Microsoft	Security Updates	Aprobado		--	Sin soporte
 33640	MS22-MAY3	2022-05 Cumulative Update for Windows 11 for x64-based Systems (KB5013943)	Microsoft	Security Updates	Aprobado		--	Con asistencia
 33874	MS22-EDGE	Microsoft Edge for chromium business (102.0.1245.39) (x64)	Microsoft	Security Updates	Aprobado		--	Sin soporte
 33923	MS22-JUN12	2022-06 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 11 for x64 (KB5013889)	Microsoft	Security Updates	Aprobado		--	Con asistencia
 33975	MS21-O365S	Update for Microsoft 365 Apps for Enterprise Semi Annual Channel for x64 2108 of version(14326.21018)	Microsoft	Security Updates	Aprobado		--	Sin soporte
 34063	MS22-EDGE	Microsoft Edge for chromium business (103.0.1264.49) (x64)	Microsoft	Security Updates	Aprobado		--	Sin soporte
 109713	MSWU-3503	2022-05 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows 11 for x64 (KB5013889)	Microsoft	Optional Updates	Aprobado		--	Con asistencia
 316162	TU-132	iCloud (7.21.0.23)	Apple	Third Party Updates	Aprobado		--	Sin soporte
 324799	TU-053	Java 8 Update 333 (8.0.3330.2) (JRE)	Oracle Corporation	Third Party Updates	Aprobado		--	Sin soporte
 324939	TU-012	Apple iTunes (X64) (12.12.4.1)	Apple	Third Party Updates	Aprobado		--	Con asistencia

ID del parche	ID de boletín	Descripción del parche	Proveedor	Tipo de parche	Aprobar estado	Comentarios	Hora de implementación	Desinstalación del parche
 325104	TU-027	Mozilla Firefox (x64) (101.0)	Mozilla	Third Party Updates	Aprobado		--	Sin soporte
325176	TU-034	Notepad++ (8.4.2)	Notepad	Third Party Updates	Aprobado		--	Con asistencia
 325285	TU-072	Adobe Acrobat Reader DC (x64) (22.001.20142)	Adobe	Third Party Updates	Aprobado		--	Sin soporte
 325540	TU-017	Google Chrome (103.0.5060.114)	Google	Third Party Updates	Aprobado		--	Sin soporte
 325541	TU-017	Google Chrome (x64) (103.0.5060.114)	Google	Third Party Updates	Aprobado		--	Sin soporte
 325589	TU-027	Mozilla Firefox (x64) (102.0.1)	Mozilla	Third Party Updates	Aprobado		--	Sin soporte
 1300536	DU-004	Intel(R) Display Audio [HDAUDIO\FUNC_01&VEN_8086&DEV_280B] (10.26.0.1)	Intel	Driver	Aprobado		--	Con asistencia
 1310821	DU-005	UHD Graphics 620 [PCI\VEN_8086&DEV_5917] (26.20.100.7926)	Intel	Driver	Aprobado		--	Con asistencia

Parches rechazados

ID del parche	Estado del parche	ID de boletín	Descripción del parche	Proveedor	Tipo de parche	Desinstalación del parche
No hay parches disponibles						

Configuraciones de seguridad a nivel de recursos

Errores de configuración del sistema

Error de configuración	Categoría	Es necesario reiniciar
Administrative Shares enabled	Share Permission Management	No obligatorio
TLSv1.1 protocol is enabled	SSL and TLS Security	Obligatorio
Geolocation is enabled to track users physical location	Chrome Security Hardening	No obligatorio
Plugins that require authorization are allowed to run without user permission	Chrome Security Hardening	No obligatorio
Secure password length is not configured (must be set to 14 characters)	Password Policy	No obligatorio
Outdated plugins are allowed to run	Chrome Security Hardening	No obligatorio
Untrusted font blocking is not enabled	OS Security Hardening	No obligatorio
Data Execution Prevention is not enabled	OS Security Hardening	Obligatorio
Structured Exception Handling Overwrite Protection (SEHOP) is not enabled	OS Security Hardening	No obligatorio
LAN Manager Authentication Level setting is not set to secure level (must be set to accept only NTLMv2 and refuse LM and NTLM)	OS Security Hardening	No obligatorio
NetBios over TCP/IP is not disabled	Legacy Protocols	No obligatorio
"Always install with elevated privileges" is not disabled	Account Privilege Management	No obligatorio
User rights granted to everyone group	Account Privilege Management	No obligatorio
Antivirus (not considering Windows Defender) not enabled	Antivirus Protection	No obligatorio
Windows Credential Guard has been found disabled	OS Security Hardening	Obligatorio
Administrator accounts are enumerated during elevation	Logon Security	No obligatorio
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Logon Security	No obligatorio
Bitlocker not enabled	BitLocker Encryption	No obligatorio

Error de configuración	Categoría	Es necesario reiniciar
User Account Control is not set to prompt administrators for consent on the secure desktop.	User Account Control	No obligatorio
Windows Defender disabled	Antivirus Protection	No obligatorio
Last signed-in username is displayed at Logon or lock screen	Logon Security	No obligatorio
User Account Control is not set to enable Admin Approval Mode for the Built-in Administrator account.	User Account Control	No obligatorio
Insecure TLSv1.0 protocol is not disabled	SSL and TLS Security	Obligatorio
Anonymized URL-keyed data collection by Google must be disabled	Chrome Security Hardening	No obligatorio
Insecure DES and 3DES cipher algorithms are not disabled	SSL and TLS Security	Obligatorio
SMB server is not configured to accept communications only from clients that perform packet signing	OS Security Hardening	No obligatorio
Websites must be prevented from accessing USB devices	Chrome Security Hardening	No obligatorio
Chrome minimum TLS/SSL connection must be configured to TLS 1.2	Chrome Security Hardening	No obligatorio
Download restrictions must be configured	Chrome Security Hardening	No obligatorio
Password history is not configured to restrict users from reusing their last 24 passwords	Password Policy	No obligatorio
Pop-ups must be blocked	Chrome Security Hardening	No obligatorio
Cloud print sharing via Chrome is not disabled	Chrome Security Hardening	No obligatorio
Inbound connection in port 135 (UDP/TCP) is not blocked in Windows firewall	Windows Firewall	No obligatorio
Inbound connection in port 137 (UDP) is not blocked in Windows firewall	Windows Firewall	No obligatorio
Inbound connection in port 138 (UDP) is not blocked in Windows firewall	Windows Firewall	No obligatorio
Inbound connection in port 139 (TCP) is not blocked in Windows firewall	Windows Firewall	No obligatorio
Inbound connection in port 445 (TCP) is not blocked in Windows firewall	Windows Firewall	No obligatorio
Cipher algorithms which do not provide perfect forward secrecy are not disabled	SSL and TLS Security	Obligatorio

Error de configuración	Categoría	Es necesario reiniciar
Chrome password manager is not disabled	Chrome Security Hardening	No obligatorio
Anonymous browser usage and crash-related data collection by Google is not disabled	Chrome Security Hardening	No obligatorio
Safe Browsing is not enabled	Chrome Security Hardening	No obligatorio
Webpages are allowed to run Flash plugins automatically	Chrome Security Hardening	No obligatorio
Firewall traversal from remote host is not disabled	Chrome Security Hardening	No obligatorio
Importing of saved passwords is not disabled	Chrome Security Hardening	No obligatorio
Chrome background apps running continuously	Chrome Security Hardening	No obligatorio
Users are allowed to bypass smartscreen filter warnings	Internet Explorer Hardening	No obligatorio
Software without valid signature are allowed to run or install through internet explorer	Internet Explorer Hardening	No obligatorio
Ensure browser history is saved	Chrome Security Hardening	No obligatorio
SMB client is not configured to communicate only with servers that perform packet signing	OS Security Hardening	No obligatorio
Folder shares with write permission are found	Share Permission Management	No obligatorio
Kerberos authentication protocol is not configured to prevent the use of DES and RC4 encryption suites	Network security	No obligatorio
Minimum session security requirement for NTLM SSP based clients are not configured	Network security	No obligatorio
Third party cookies must be blocked	Chrome Security Hardening	No obligatorio
System is using default cipher suites	SSL and TLS Security	Obligatorio
Insecure NULL ciphers are not disabled	SSL and TLS Security	Obligatorio
Prompting clients for passwords upon remote desktop connection is disabled	Password Policy	No obligatorio
Passwords are allowed to be saved in the Remote Desktop Client	Password Policy	No obligatorio
Minimum session security requirement for NTLM SSP based servers are not configured	Network security	No obligatorio

Error de configuración del servidor web

Error de configuración del servidor web	Categoría	Ruta del archivo
No se han detectado errores de configuración de servidor web en los criterios especificados		

Excluded Misconfiguration

Error de configuración	Categoría	Reason for exclusion
No Misconfigurations are excluded		

Excluded Hardening

Error de configuración del servidor web	Categoría	Ruta del archivo	Reason for exclusion
No Web server misconfigurations are excluded			