Resource Health Summary

August 14,2022 05:48 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	:	LSALASW10
Sistema operativo	:	Windows 11 Professional Edition (x64)
Paquete de servicio	:	Windows 11 Version 21H2 (x64)
Idioma	:	Español
Estado Correcto	:	Vulnerable
Hora del último parche	:	--
Estado de último análisis	:	Análisis finalizado
Dirección IP	:	192.168.35.11
Dominio	:	WORKGROUP
Oficina remota	:	Local Office
Usuarios conectados	:	Lenovo
Último análisis correcto	:	jul 13, 2022 11:14 AM
Hora del último inicio	:	jul 13, 2022 01:00 AM

Es necesario reiniciar	:	No

Table of Contents

Configuraciones de seguridad a nivel de recursos

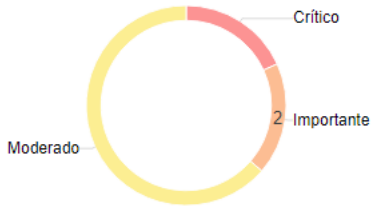
Acerca de

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

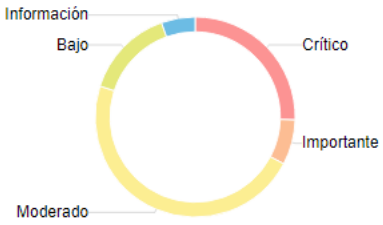
Este informe le ayuda a aliviar la tensión al proporcionarle la lista de parches, sistemas, vulnerabilidades, errores de configuración y otras amenazas sobre los que debe actuar de inmediato. El resumen de estado de los parches le ha proporcionado una vista de nivel superior de los parches que faltan 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



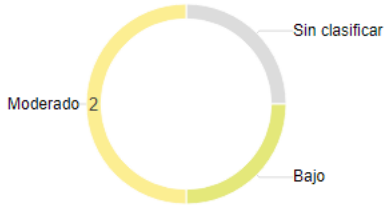
Errores de configuración del sistema



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
Vulnerabilities CVE-2020-14577,CVE-2020-14583,CVE-2020-14593,CVE-2020-14621 are affected in Java SE, Java SE Embedded 8u251	No disponible	Disponible	10.0	7.5	jul 24, 2020	jul 24, 2020	jul 24, 2020	Windows
Multiple vulnerabilities affected in Java SE, Java SE Embedded 14.0.1; Java SE Embedded: 8u251	No disponible	Disponible	10.0	7.5	jul 24, 2020	jul 24, 2020	jul 24, 2020	Windows
Vulnerabilities CVE-2020-14664 are affected in Java SEJava SE: 8u251	No disponible	Disponible	8.5	5.1	jul 24, 2020	jul 24, 2020	jul 24, 2020	Windows
Multiple vulnerabilities affected in Java SE 8u301	No disponible	No disponible	8.7	7.5	oct 20, 2021	oct 20, 2021	oct 20, 2021	Windows
Vulnerabilities CVE-2020-14578,CVE-2020-14579 are affected in Java SE, Java SE Embedded 8u251; Java SE Embedded: 8u251	No disponible	Disponible	3.6	4.3	jul 24, 2020	jul 24, 2020	jul 24, 2020	Windows
Vulnerabilities CVE-2020-14556,CVE-2020-14581 are affected in Java SE, Java SE EmbeddedJava SE: 8u251	No disponible	Disponible	4.9	5.8	jul 24, 2020	jul 24, 2020	jul 24, 2020	Windows
Multiple vulnerabilities affected in Java SE, Java SE Embedded 15; Java SE Embedded: 8u261	No disponible	No disponible	5.7	6.8	oct 22, 2020	oct 22, 2020	oct 22, 2020	Windows

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 Java SE, Java SE Embedded 8u261	No disponible	No disponible	5.7	6.8	oct 22, 2020	oct 22, 2020	oct 22, 2020	Windows
Vulnerabilities CVE-2020-14803 are affected in \nJava Runtime Environment 1.8	No disponible	No disponible	5.5	5.0	may 25, 2021	may 25, 2021	may 25, 2021	Windows
Multiple vulnerabilities affected in Oracle Java SE 8u311	No disponible	Disponible	5.5	5.0	ene 19, 2022	ene 19, 2022	ene 19, 2022	Windows
Multiple vulnerabilities affected in Oracle Java SE 8u321	No disponible	Disponible	6.4	6.4	abr 20, 2022	abr 20, 2022	abr 20, 2022	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
No hay resultados disponibles que coincidan con estos criterios		

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
Teamviewer 15	TeamViewer

Final de la vida

Nombre del software	Proveedor	Fecha de vencimiento	Días para que caduque
Internet Explorer 11 for x64	Microsoft	jun 15, 2022	Vencida

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
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
325443	TU-063	WinSCP (5.21.1)	WinSCP	Third Party Updates	Aprobado		--	Con asistencia
325488	TU-057	Teamviewer 15 (15.31.5)	TeamViewer	Third Party Updates	Aprobado		--	Sin soporte
1312826	DU-003	Ice Lake-LP PCH CNVi WiFi[PCI\VEN_8086&DEV_34F0] (22.110.1.1)	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
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
33891	MS22-JUN3	2022-06 Cumulative Update for Windows 11 for x64-based Systems (KB5014697) (CVE-2022-30190)	Microsoft	Security 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
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
324799	TU-053	Java 8 Update 333 (8.0.3330.2) (JRE)	Oracle Corporation	Third Party Updates	Aprobado		--	Sin soporte
325133	TU-058	FileZilla Client (x64) (3.60.1)	Tim Kosse	Third Party Updates	Aprobado		--	Con asistencia
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

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
Geolocation is enabled to track users physical location	Chrome Security Hardening	No obligatorio
TLSv1.1 protocol is enabled	SSL and TLS Security	Obligatorio
Administrative Shares enabled	Share Permission Management	No obligatorio
Structured Exception Handling Overwrite Protection (SEHOP) is not enabled	OS Security Hardening	No obligatorio
Data Execution Prevention is not enabled	OS Security Hardening	Obligatorio
Untrusted font blocking is not enabled	OS Security Hardening	No obligatorio
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Logon Security	No obligatorio
"Always install with elevated privileges" is not disabled	Account Privilege Management	No obligatorio
NetBios over TCP/IP is not disabled	Legacy Protocols	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
Windows Credential Guard has been found disabled	OS Security Hardening	Obligatorio
Administrator accounts are enumerated during elevation	Logon Security	No obligatorio
User rights granted to everyone group	Account Privilege Management	No obligatorio
Bitlocker not enabled	BitLocker Encryption	No obligatorio
Outdated plugins are allowed to run	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
User Account Control is not set to prompt administrators for consent on the secure desktop.	User Account Control	No obligatorio

Error de configuración	Categoría	Es necesario reiniciar
Insecure TLSv1.0 protocol is not disabled	SSL and TLS Security	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
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
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
Chrome background apps running continuously	Chrome Security Hardening	No obligatorio
Cipher algorithms which do not provide perfect forward secrecy 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
SMB client is not configured to communicate only with servers that perform packet signing	OS Security Hardening	No obligatorio
Ensure browser history is saved	Chrome Security Hardening	No obligatorio
Importing of saved passwords 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
Chrome password manager is not disabled	Chrome Security Hardening	No obligatorio
Cloud print sharing via Chrome is not disabled	Chrome Security Hardening	No obligatorio
Pop-ups must be blocked	Chrome Security Hardening	No obligatorio
Chrome minimum TLS/SSL connection must configured to TLS 1.2	Chrome Security Hardening	No obligatorio
Websites must be prevented from accessing USB devices	Chrome Security Hardening	No obligatorio
Anonymized URL-keyed data collection by Google must be disabled	Chrome Security Hardening	No obligatorio

Error de configuración	Categoría	Es necesario reiniciar
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
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
Safe Browsing is not enabled	Chrome Security Hardening	No obligatorio
Insecure DES and 3DES cipher algorithms are not disabled	SSL and TLS Security	Obligatorio
Prompting clients for passwords upon remote desktop connection is disabled	Password Policy	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 servers are not configured	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
Passwords are allowed to be saved in the Remote Desktop Client	Password Policy	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			