BAFING

Fecha:		**09/10/2024**		
Detalle reportado:		**Boletín – Vulnerabilidades en productos de Microsoft**		
Caso de uso:		**CUS_GRL_04_Boletines**		
Severidad:	⚠	Riesgo grave, requiere atención de alta prioridad.		X
	⚠	Riesgo intermedio, validación de problemas menores.		
	⚠	No hay problemas graves. Alerta informativa.		
Estado:		**Alertado**		

Descripción

Boletín – Vulnerabilidades en productos de Microsoft

Microsoft publicó recientemente su actualización de seguridad de octubre de 2024, la cual incluye parches para 118 vulnerabilidades que afectan a una variedad de productos y servicios. A continuación, se brindan detalles de algunas de las vulnerabilidades publicadas:

CVE-2024-43468: Vulnerabilidad en Microsoft Configuration Manager permite ejecución de código arbitrario**. - (CRÍTICA)**

Se detectó una vulnerabilidad de neutralización incorrecta de elementos especiales en Microsoft Configuration Manager permite que un atacante no autenticado envíe solicitudes especialmente diseñadas al entorno de destino, los cuales se procesarán de manera insegura, logrando la ejecución de código arbitrario en el servidor o base de datos subyacente.

Versiones afectadas:

- Microsoft Configuration Manager 2403 en versiones previas a 5.00.9128
- Microsoft Configuration Manager 2309 en versiones previas a 5.00.9122
- Microsoft Configuration Manager 2303 en versiones previas a 5.00.9106

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de Microsoft Configuration Manager. De ser el caso, aplicar las actualizaciones o parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43468

CVE-2024-38124: Vulnerabilidad en Windows Netlogon permite elevación de privilegios**. - (CRÍTICA)**

Una vulnerabilidad de autenticación incorrecta en Microsoft Windows Netlogon puede ocasionar que un atacante autenticado con acceso LAN pueda obtener privilegios de administrador de dominio y comprometer el dominio controlado.

Versiones afectadas:

- Microsoft Windows Server 2022 edición 23H2 en versiones previas a 10.0. 25398.1189
- Microsoft Windows Server 2022 en versiones previas a 10.0.20348.2762
- Microsoft Windows Server 2019 en versiones previas a 10.0.17763.6414
- Microsoft Windows Server 2016 en versiones previas a 10.0.14393.7428
- Microsoft Windows Server 2012 R2 en versiones previas a 6.3.9600.22221
- Microsoft Windows Server 2012 en versiones previas a 6.2.9200.25118
- Microsoft Windows Server 2008 R2 en versiones previas a 6.1.7601.27366
- Microsoft Windows Server 2008 en versiones previas a 6.0.6003.22918

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de los productos reportados. De ser el caso, aplicar las actualizaciones o parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38124

CVE-2024-43582: Vulnerabilidad en servidor RDP de Windows permite ejecución remota de código**. - (CRITICA)**

Un uso después de la liberación de la memoria en el servidor RDP de Windows permite que un atacante no autenticado, al enviar paquetes malformados a un host RPC, pueda ejecutar código arbitrario en el lado del servidor con los mismos permisos que el servicio RPC.

Versiones afectadas:

- Microsoft Windows Server 2022 edición 23H2 en versiones previas a 10.0. 25398.1189
- Microsoft Windows Server 2022 en versiones previas a 10.0.20348.2762
- Microsoft Windows Server 2019 en versiones previas a 10.0.17763.6414
- Microsoft Windows 11 version 21H2 en versiones previas a 10.0.22000.3260
- Microsoft Windows 11 version 24H2 en versiones previas a 10.0.26100.2033
- Microsoft Windows 11 version 23H2 en versiones previas a 10.0.22631.4317
- Microsoft Windows 11 version 22H2 en versiones previas a 10.0.22621.4317
- Microsoft Windows 10 version 22H2 en versiones previas a 10.0.19045.5011
- Microsoft Windows 10 version 21H2 en versiones previas a 10.0.19044.5011
- Microsoft Windows 10 version 1809 en versiones previas a 10.0.17763.6414

Recomendación:

Se recomienda validar si la organización cuenta con las versiones vulnerables de los productos reportados. De ser el caso, aplicar las actualizaciones o parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43582

CVE-2024-43572: Vulnerabilidad en Microsoft Management Console permite ejecución remota de código**. - (ALTA)**

Se detectó una vulnerabilidad de neutralización incorrecta en Microsoft Management Console puede generar que un atacante ejecute código arbitrario, al lograr que una víctima descargue y abra un archivo MSC especialmente diseñado. Microsoft es consciente de la existencia de un exploit para la vulnerabilidad.

CVE-2024-43573: Vulnerabilidad en la plataforma MSHTML de Windows permite un ataque de spoofing**. - (MEDIA)**

Una vulnerabilidad de neutralización incorrecta de la entrada durante la generación de páginas web puede ser aprovechada por un atacante para generar ataques de spoofing. Microsoft es consciente de la existencia de un exploit para la vulnerabilidad.

Versiones afectadas:

- Microsoft Windows Server 2022 edición 23H2 en versiones previas a 10.0. 25398.1189
- Microsoft Windows Server 2022 en versiones previas a 10.0.20348.2762
- Microsoft Windows Server 2019 en versiones previas a 10.0.17763.6414
- Microsoft Windows Server 2012 R2 en versiones previas a 6.3.9600.22221
- Microsoft Windows Server 2012 en versiones previas a 6.2.9200.25118
- Microsoft Windows Server 2008 R2 en versiones previas a 6.1.7601.27366
- Microsoft Windows Server 2008 en versiones previas a 6.0.6003.22918
- Microsoft Windows 11 version 21H2 en versiones previas a 10.0.22000.3260
- Microsoft Windows 11 version 24H2 en versiones previas a 10.0.26100.2033
- Microsoft Windows 11 version 23H2 en versiones previas a 10.0.22631.4317
- Microsoft Windows 11 version 22H2 en versiones previas a 10.0.22621.4317
- Microsoft Windows 10 version 22H2 en versiones previas a 10.0.19045.5011
- Microsoft Windows 10 version 21H2 en versiones previas a 10.0.19044.5011
- Microsoft Windows 10 version 1809 en versiones previas a 10.0.17763.6414
- Microsoft Windows 10 version 1607 en versiones previas a 10.0.14393.7428
- Microsoft Windows 10 en versiones previas a 10.0.10240.20796

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de los productos reportados. De ser el caso, aplicar las actualizaciones o parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

BAFING

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573

+51 1 225 9900
info@bafing.com
www.bafing.com
Bafing
Av. Del Parque Sur 560, San Borja, Lima,Perú