
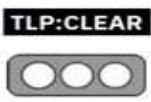


Nro. Alerta:	AL-2023-027	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	26-junio-2023	<b>Vulnerabilidad MOVEit Transfer</b>	Pág.: 1 of 5

## I. DATOS GENERALES:

**Clase de alerta:** Vulnerabilidad  
**Tipo de incidente:** Ejecución remota de código (RCE)  
**Nivel de riesgo:** Crítico

## II. ALERTA

Una vulnerabilidad de día cero de inyección SQL en la solución de transferencia de archivos administrados (MFT) MOVEit Transfer que ha sido un objetivo activo desde finales de mayo de 2023. La explotación exitosa podría conducir a la ejecución remota de código (RCE), lo que permitiría a los atacantes no autenticados, ejecutar código arbitrario para realizar actividades maliciosas, como deshabilitar soluciones antivirus (AV) o implementar cargas útiles de malware.



Figura No. 1.- Ilustración asociada a MOVEit Transfer

Fuente: <https://thehackernews.com/2023/06/moveit-transfer-under-attack-zero-day.html>

## III. INTRODUCCIÓN

El 31 de mayo de 2023, *Progress Software Corporation* publicó un aviso de seguridad advirtiendo a los clientes sobre una vulnerabilidad en las instancias locales y con acceso a Internet de su solución *MOVEit Transfer*, que podría conducir a una escalada de privilegios y un posible acceso no autorizado a los sistemas; el 2 de junio de 2023 a esta vulnerabilidad se le asignó el CVE-2023-34362, y ha sido explotada desde el 27 de mayo de 2023, pero es posible que los actores de amenazas hayan comenzado a experimentar su explotación desde 2021 .

La vulnerabilidad de MOVEit Transfer, CVE-2023-34362, cubre múltiples fallas que un atacante puede encadenar para lograr la Ejecución remota de código RCE con privilegios elevados. La primera parte de la cadena de explotación utiliza la inyección de SQL para obtener un token API de administrador de sistemas. Ese token se puede usar para llamar a una función que, no valida correctamente la entrada, lo que permite la ejecución remota de código.



<https://www.ecucert.gob.ec>



@EcuCERT\_EC

Agencia de Regulación y Control de las Telecomunicaciones

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel


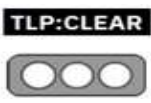
Código postal: 170501 / Quito-Ecuador

Teléfono: 593-2 2271 180

[www.arcotel.gob.ec](http://www.arcotel.gob.ec)



República del Ecuador

Nro. Alerta:	AL-2023-027	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	26-junio-2023	<b>Vulnerabilidad MOVEit Transfer</b>	V 1.1 Pág.: 2 of 5

El 9 de junio de 2023, se asignó una segunda vulnerabilidad, CVE-2023-35036, y *Progress Software* lanzó parches destinados a mitigar múltiples partes de la explotación que inicialmente se descubrió en el CVE-2023-34362, el 15 de junio de 2023 se identificó otra vulnerabilidad bajo el CVE-2023-35708, *Progress Software* lanzó parches instalables para corregir esta vulnerabilidad.

## EXPLOTACION

El grupo de *ransomware Clop* emitió una declaración pública en su sitio de Tor, asumiendo la responsabilidad de los ataques y amenazando con publicar los datos de las víctimas si no se paga la demanda de extorsión. En esta actividad, el grupo de ransomware Clop explotó la CVE-2023-34362 para instalar un shell web previamente desconocida ahora denominado "LemurLoot". (Talos, 2023)

*LemurLoot* está diseñado para extraer datos y ejecutarse en sistemas que ejecutan *MOVEit Transfer*. La shell web se implementa con un formato Identificador Único Global (GUID) de 36 caracteres codificado para autenticar las solicitudes de conexión entrantes desde el atacante. El valor del código de autenticación debe estar presente en el campo de encabezado "X-siLock-Comment", si el valor es correcto, la shell web confirma que puede aceptar tareas y se conecta a un servidor SQL controlado por un atacante.

## IV. VECTOR DE ATAQUE:

Todas las versiones de *MOVEit Transfer*, anteriores al 31 de mayo de 2023, son vulnerables a CVE-2023-34362. A continuación, una tabla con las versiones corregidas:

Versión afectada	Version Corregida (full installer)	Documentación
MOVEit Transfer 2023.0.x (15.0.x)	MOVEit Transfer 2023.03 (15.0.3)	Documentación de actualización de MOVEit 2023
MOVEit Transfer 2022.1.x (14.1.x)	MOVEit Transfer 2022.1.7 (14.1.7)	Documentación de actualización de MOVEit 2022
MOVEit Transfer 2022.0.x (14.0.x)	MOVEit Transfer 2022.0.6 (14.0.6)	
MOVEit Transfer 2021.1.x (13.1.x)	MOVEit Transfer 2021.1.6 (13.1.6)	Documentación de actualización de MOVEit 2021
MOVEit Transfer 2021.0.x (13.0.x)	MOVEit Transfer 2021.0.8 (13.0.8)	
MOVEit Transfer 2020.1.x (12.1)	Debe actualizar al menos a 2020.1.6 y luego aplicar DLL provistas por el proveedor	Corrección para MOVEit Transfer 2020.1 (12.1)



<https://www.ecucert.gob.ec>



@EcuCERT\_EC

Agencia de Regulación y Control de las Telecomunicaciones

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel


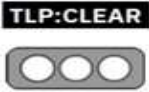
Código postal: 170501 / Quito-Ecuador

Teléfono: 593-2 2271 180

[www.arcotel.gob.ec](http://www.arcotel.gob.ec)



República del Ecuador

Nro. Alerta:	AL-2023-027	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	26-junio-2023	<b>Vulnerabilidad MOVEit Transfer</b>	Pág.: 3 of 5

MOVEit Transfer 2020.0.x (12.0) or older	DEBE actualizar a una versión soportada	Consulte la Guía de actualización y migración de MOVEit Transfer
MOVEit Cloud	Prod: 14.1.6.97 or 14.0.5.45 Test: 15.0.2.39	Todos los sistemas MOVEit Cloud están completamente parcheados.

**Tabla No. 1.-** Versiones afectadas de MOVEit Transfer

Fuente: <https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023>

## V. IMPACTO:

Exfiltración de información  
Acceso no autorizado a la base de datos de MOVEit Transfer

## VI. INDICADORES DE COMPROMISO

Hashes para LEMURLOOT y web Shell:

```
0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9
0ea05169d111415903a1098110c34cdbbd390c23016cd4e179dd9ef507104495
110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286
1826268249e1ea58275328102a5a8d158d36b4fd312009e4a2526f0bfb30de2
2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
2ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59
348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d
387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a
38e69f4a6d2e81f28ed2dc6df0daf31e73ea365bd2cfc90ebc31441404cca264
```

**Mas información de IoCs. (CISA, 2023)**

## VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Aplicar las actualizaciones provistas por el proveedor *Progress* del producto *MOVEit Transfer* y descargarlas desde sitios oficiales.
- Eliminar archivos y cuentas de usuario no autorizados y restablecer las credenciales de la cuenta de servicio.
- Actualizar las reglas del firewall, para permitir únicamente conexiones a la infraestructura de MOVEit Transfer desde direcciones IP conocidas, configurar el firewall del sistema para bloquear el tráfico malicioso.
- Actualizar las políticas de acceso remoto para permitir solo conexiones entrantes desde direcciones IP conocidas y confiables, y usar control de acceso basado en certificados.
- Habilitar la autenticación multifactor.



<https://www.ecucert.gob.ec>



@EcuCERT\_EC

**Agencia de Regulación y Control de las Telecomunicaciones**

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel


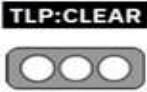
Código postal: 170501 / Quito-Ecuador

Teléfono: 593-2 2271 180

[www.arcotel.gob.ec](http://www.arcotel.gob.ec)



República del Ecuador

Nro. Alerta:	AL-2023-027	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	26-junio-2023	<b>Vulnerabilidad MOVEit Transfer</b>	Pág.: 4 of 5

- Consultar los avisos para CVE-2023-34362, CVE-2023-35036 y CVE-2023-35708 para aplicar los parches correspondientes.
- Utilizar la administración de la superficie de ataque para identificar los activos que podrían estar expuestos a los actores de amenazas y actuar con precaución al aplicar los parches de seguridad más recientes siempre que sea posible.
- Mantener actualizado el software del sistema operativo y las aplicaciones, pero actuar con precaución al aplicar los parches de seguridad, y utilizar los más recientes siempre que sea posible.
- Instalar un software antivirus y mantenerlo actualizado.
- Monitorear de manera proactiva las relaciones de ejecución de procesos anormales y tomar medidas preventivas para evitar actividades como la exfiltración de información.
- Analizar solicitudes web sospechosas: Webshell relacionado con MOVEit Exploit

Con estas recomendaciones de seguridad, se puede minimizar las posibilidades de ser una víctima, las recomendaciones no garantizan la seguridad, pero ayudan a reducir el riesgo.

## VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

## IX. REFERENCIAS:

- CISA. (2023, junio 7). #StopRansomware: CLOP Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability. Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a>
- CISA. (s. f.). *Known Exploited Vulnerabilities Catalog*. Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Condon, C. (2023). Rapid7 Observed Exploitation of Critical MOVEit Transfer Vulnerability. *Rapid7*. <https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-moveit-transfer-vulnerability/>
- NVD - CVE-2023-34362. (s. f.). <https://nvd.nist.gov/vuln/detail/CVE-2023-34362>



<https://www.ecucert.gob.ec>



@EcuCERT\_EC

**Agencia de Regulación y Control de las Telecomunicaciones**

Dirección: Av. Amazonas N40-71 y Gaspar de Villarreal


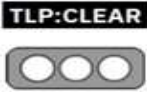
Código postal: 170501 / Quito-Ecuador

Teléfono: 593-2 2271 180

[www.arcotel.gob.ec](http://www.arcotel.gob.ec)



República del Ecuador

Nro. Alerta:	AL-2023-027	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	26-junio-2023	<b>Vulnerabilidad MOVEit Transfer</b>	Pág.: 5 of 5

- *Progress Customer Community*. (s. f.-a). <https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023>
- *Progress Customer Community*. (s. f.-b). <https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023>
- *Progress Customer Community*. (s. f.-c). <https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-2023-35036-June-9-2023>
- *Progress Customer Community*. (s. f.-d). <https://community.progress.com/s/global-search/%40uri#q=MOVEit%20transfer&t=All&sort=relevancy>
- Talos, C. (2023a). Active exploitation of the MOVEit Transfer vulnerability — CVE-2023-34362 — by Clop ransomware group. *Cisco Talos Blog*. <https://blog.talosintelligence.com/active-exploitation-of-moveit/>
- Talos, C. (2023b). Active exploitation of the MOVEit Transfer vulnerability — CVE-2023-34362 — by Clop ransomware group. *Cisco Talos Blog*. <https://blog.talosintelligence.com/active-exploitation-of-moveit/>
- The Hacker News. (s. f.). *MOVEit Transfer Under Attack: Zero-Day Vulnerability Actively Being Exploited*. <https://thehackernews.com/2023/06/moveit-transfer-under-attack-zero-day.html>



<https://www.ecucert.gob.ec>



@EcuCERT\_EC

**Agencia de Regulación y Control de las Telecomunicaciones**

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel

Código postal: 170501 / Quito-Ecuador

Teléfono: 593-2 2271 180

[www.arcotel.gob.ec](http://www.arcotel.gob.ec)



República del Ecuador