

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

TROPIGAS

November 11, 2026



©2023. GLESEC. All Rights Reserved.

TROPIGAS 11/11/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "SEPTIEMBRE 2026" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, Amenazas, Activos, Cumplimiento, Validación de Ciberseguridad y Acceso.

SOBRE ESTE INFORME

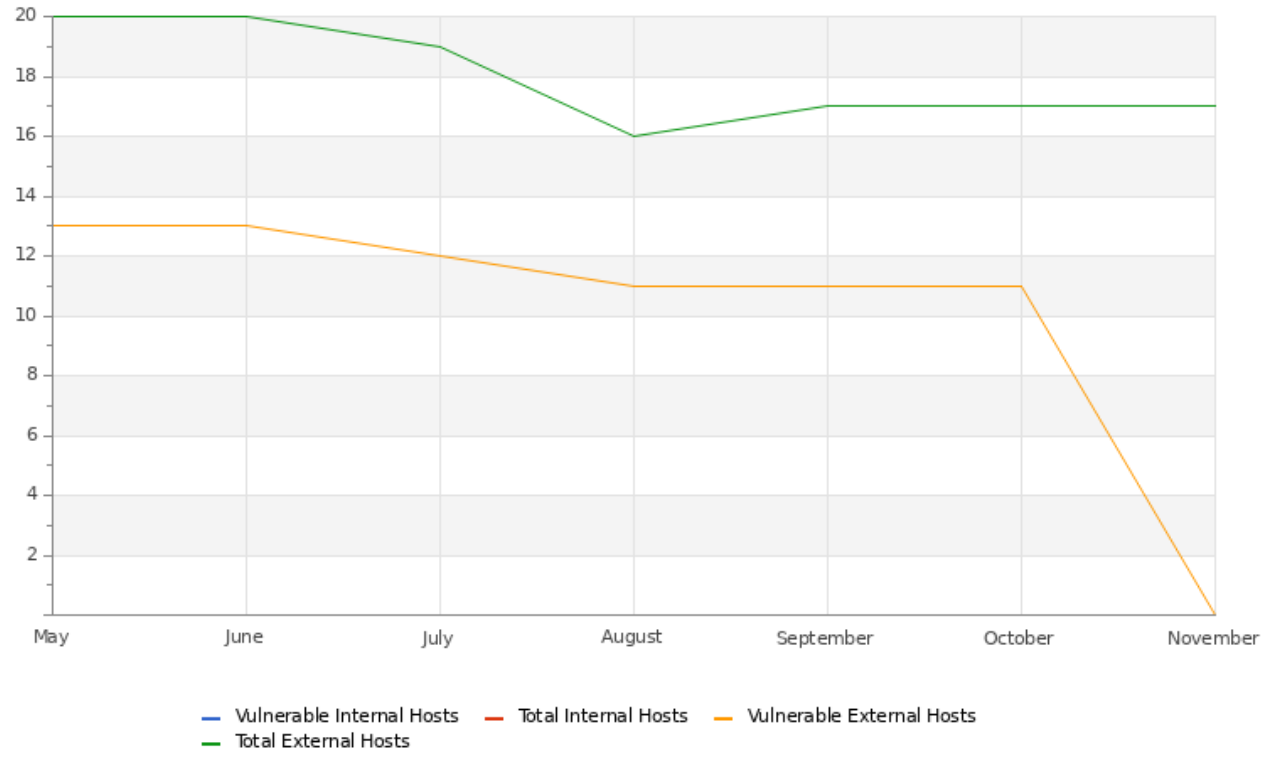
El propósito de este documento es informar sobre el estado" de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TROPIGAS 11/11/2026

Hosts & Vulnerable Hosts In Last 6 Months



Durante septiembre se observa un ligero incremento en la cantidad de sistemas descubiertos y en el total de hallazgos de seguridad respecto al mes anterior. A través de MSS-EASM, se identificaron 17 sistemas expuestos a Internet, de los cuales 11 presentan vulnerabilidades activas, frente a los 16 sistemas y 11 hosts vulnerables registrados en agosto. Asimismo, se identificaron 28 hallazgos, en comparación con los 25 reportados en agosto. Esta variación incluye una nueva vulnerabilidad de severidad alta asociada a Microsoft Exchange, mientras que un hallazgo de severidad media identificado en agosto dejó de presentarse. Las principales oportunidades de mejora continúan relacionadas con protocolos obsoletos, certificados digitales, servicios inseguros y configuraciones de seguridad web. Esta evolución evidencia un incremento en la superficie de exposición y la aparición de riesgos de mayor severidad, por lo que resulta necesario reforzar las acciones de remediación y seguimiento, priorizando la atención de la vulnerabilidad alta identificada.

Total Attacks Successfully Blocked

40559197

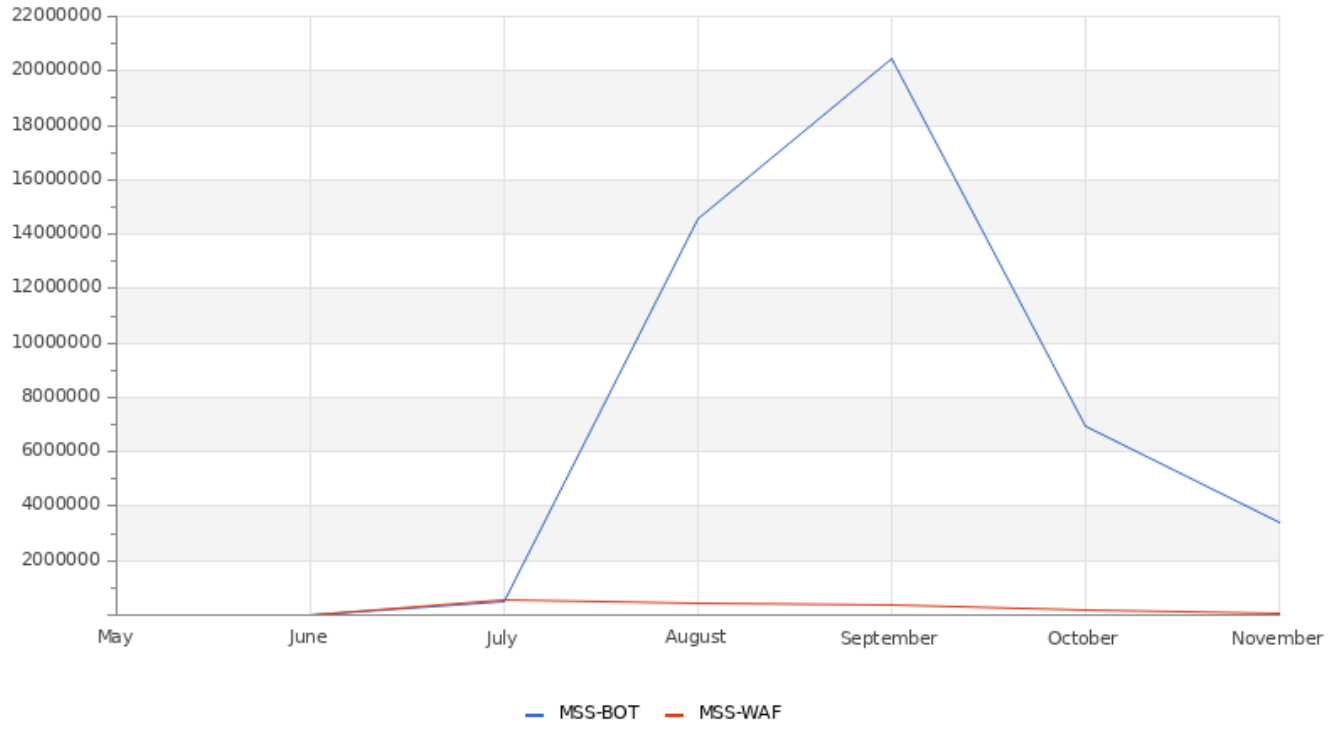
Durante septiembre de 2026, MSS-WAF Cloud registró 437,738 eventos de seguridad, frente a los 545,594 eventos registrados en agosto, lo que representa una reducción aproximada del 19.77 % en el volumen de eventos recibidos. La actividad observada estuvo asociada a los controles de seguridad del servicio WAF, que permitieron identificar y gestionar solicitudes maliciosas y tráfico dirigido contra las aplicaciones protegidas. Del total de eventos registrados en septiembre, 362,340 fueron bloqueados (82.77 %), 54,794 fueron modificados (12.52 %) y 20,604 fueron reportados (4.71 %). Esta distribución evidencia que la acción predominante fue el bloqueo, demostrando que la mayor parte de la actividad identificada recibió una acción preventiva por parte del WAF. Aunque se mantiene una reducción en el volumen de eventos respecto a agosto, resulta importante continuar monitoreando el comportamiento de los controles y profundizar en el análisis de los eventos reportados para identificar posibles oportunidades de mejora y mantener la efectividad de la protección sobre las aplicaciones y servicios de la organización.

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL

Critical Attacks Successfully Blocked

875260

Attacks Successfully Blocked



Durante septiembre de 2026, el análisis conjunto de los componentes WAF y BOT permitió identificar diferencias relevantes en el tratamiento aplicado al tráfico observado. En WAF se registraron 437,738 eventos de seguridad, de los cuales el 82.77 % fueron bloqueados, el 12.52 % modificados y el 4.71 % reportados, evidenciando que la acción predominante fue el bloqueo. No obstante, dentro de los eventos registrados como Reported se identificaron técnicas relevantes como Code Injection, Remote File Inclusion, Path Traversal, Cross-Site Scripting, SQL Injection y Server-Side Request Forgery, dirigidas contra diferentes aplicaciones protegidas.

Por su parte, el componente BOT registró 72,375 solicitudes bloqueadas durante septiembre, frente a 76,719 en agosto, lo que representa una reducción del 5.66 %. En conjunto, los resultados reflejan que ambos componentes mantuvieron acciones de protección sobre el tráfico dirigido a los servicios de la organización, aunque es importante continuar monitoreando las técnicas identificadas en WAF y el comportamiento de las solicitudes BOT para mantener la efectividad de los controles de seguridad.

©2023. GLESEC. All Rights Reserved. PROPRIETARY & CONFIDENTIAL
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TROPIGAS 11/11/2026

Vulnerability Metric

3

El análisis de la superficie externa durante septiembre identificó 17 sistemas expuestos a Internet, de los cuales 11 presentan vulnerabilidades activas, con un total de 28 hallazgos, frente a los 16 sistemas y 25 vulnerabilidades externas registrados en agosto. Aunque la cantidad de activos con vulnerabilidades se mantuvo estable, se observa un incremento de tres hallazgos respecto al mes anterior. A diferencia de agosto, durante septiembre se identificó una vulnerabilidad de severidad alta asociada a Microsoft Exchange, mientras que un hallazgo de severidad media dejó de presentarse. Las principales debilidades continúan relacionadas con protocolos obsoletos, certificados digitales, servicios inseguros y configuraciones de seguridad web. La aparición de una vulnerabilidad de mayor severidad representa un cambio relevante en el nivel de riesgo de la superficie externa, por lo que se recomienda priorizar su remediación y mantener las acciones de seguimiento sobre las demás exposiciones identificadas.

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

©2023. GLESEC. All Rights Reserved.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500



TLP:AMBER

BOARDROOM EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

©2023. GLESEC. All Rights Reserved.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500