USTIC-AV 14/22. Vulnerabilidad crítica en firewalls Fortigate (10/10/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones **avisa de la publicación de una vulnerabilidad crítica que afecta a los firewalls FortiGate, que podría permitir que un atacante realice acciones no autorizadas.**

Detalle

Fortinet ha publicado un comunicado en el que advierte sobre un fallo crítico de seguridad que **afecta a los firewalls Fortigate** y a los servidores proxy web FortiProxy .

Identificada como **CVE-2022-40684,** esta **vulnerabilidad de omisión de autenticación crítica** recibió una puntuación CVSSv3 de 9,6 sobre 10. Al enviar solicitudes *http* o *https* especialmente diseñadas a un objetivo vulnerable, **un atacante remoto con acceso a la interfaz de administración podría realizar operaciones de administrador.**

En este momento, no hay información sobre si esta vulnerabilidad está siendo explotada activamente, pero debido a su gravedad, rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas.

Recursos Afectados

El problema afecta a las siguientes versiones:

- ***FortiOS***: De 7.0.0 a 7.0.6 y de 7.2.0 a 7.2.1

Recomendaciones Actualizadas (10/10/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas:

Mitigación

1º. Solución a las vulnerabilidades:

Actualizar los dispositivos vulnerables **a las versiones 7.0.7 o 7.2.2** de *FortiOS*

2º. *Workaround* de las vulnerabilidades:

La empresa también proporciona una solución alternativa para aquellos que no pueden implementar actualizaciones de seguridad de inmediato. Para evitar que los atacantes remotos eludan la autenticación e inicien sesión en implementaciones vulnerables de FortiGate y FortiProxy, se deben limitar las direcciones IP que pueden llegar a la interfaz administrativa mediante una política local.

Referencias

- https://www.tenable.com/blog/cve-2022-40684-critical-authentication-bypass-in-fortios-and-fortiproxy
- https://docs.fortinet.com/document/fortigate/7.2.2/fortios-release-notes/289806/resolved-issues
- https://docs.fortinet.com/document/fortiproxy/7.0.7/release-notes/987706/what-s-new

---

En caso de haber detectado la explotación de esta vulnerabilidad :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indic ando en el *Asunto: [Compromiso Fortigate1022]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud