USTIC-ALERT 04/22. Vulnerabilidad crítica activamente explotada en firewalls Fortigate (14/12/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el CCN-CERT, del Centro Criptológico Nacional, **alerta** de la publicación de una **vulnerabilidad crítica** que afecta a los **firewalls FortiGate, que podría permitir a un atacante no autenticado** la **ejecución remota de código arbitrario** o **comandos** mediante determinadas peticiones.

Detalle

Fortinet ha publicado un comunicado en el que advierte de un fallo crítico de seguridad en FortiOS SSL-VPN que puede permitir que un atacante remoto no autenticado ejecute código o comandos arbitrarios a través de solicitudes diseñadas específicamente.

El fabricante ha admitido que esta **vulnerabilidad de desbordamiento de búfer crítica**, identificada como **CVE-2022-42475** y que recibió una puntuación CVSSv3 de 9,3 sobre 10, **está siendo activamente explotada** y recomienda validar inmediatamente los sistemas contra los siguientes indicadores de compromiso que facilitan en su sitio web:

- **Múltiples entradas de registro con:**
  - `Logdesc="Application crashed" and msg="[...] application:sslvpnd,[...], Signal 11 received, Backtrace: [...]“`
- **Presencia de los siguientes artefactos en el sistema de archivos:**
  - `/data/lib/libips[.]bak`
  - `/data/lib/libgif[.]so`
  - `/data/lib/libiptcp[.]so`
  - `/data/lib/libipudp[.]so`
  - `/data/lib/libjepg[.]so`
  - `/var/[.]sslvpnconfigbk`
  - `/data/etc/wxd[.]conf`
  - `/flash`
- **Conexiones a direcciones IP sospechosas desde FortiGate:**
  - `188[.]34.130[.]40:444`
  - `103[.]131.189[.]143:30080,30081,30443,20443`
  - `192[.]36.119[.]61:8443,444`
  - `172[.]247[.]168.153:8033`

De acuerdo con la información publicada, se trata de un escenario de riesgo, por lo que se ruega se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a esta vulnerabilidad.

Recursos Afectados

El problema afecta a las siguientes versiones:

- **FortiOS** versión 7.0.0 a 7.0.8
- **FortiOS** versión 6.4.0 a 6.4.10
- **FortiOS** versión 6.2.0 a 6.2.11
- **FortiOS** versión 6.0.0 a 6.0.15
- **FortiOS** versión 5.6.0 a 5.6.14
- **FortiOS** versión 5.4.0 a 5.4.13
- **FortiOS** versión 5.2.0 a 5.2.15
- **FortiOS** versión 5.0.0 a 5.0.14
- **FortiOS-6K7K** versión 7.0.0 a 7.0.7
- **FortiOS-6K7K** versión 6.4.0 a 6.4.9
- **FortiOS-6K7K** versión 6.2.0 a 6.2.11
- **FortiOS-6K7K** versión 6.0.0 a 6.0.14

Recomendaciones Actualizadas (14/12/2022)

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 la vulnerabilidad:

- **Actualizar** los dispositivos vulnerables **a las siguientes versiones** de ***FortiOS: 7.2.3, 7.0.9, 6.4.11, 6.2.12 o superiores*** **y** a las siguientes versiones **de FortiOS-6K7K*: 7.0.8, 6.4.10, 6.2.12 y 6.0.15 o superiores.***

2º. *Workaround de la* vulnerabilidad:

- La empresa también proporciona una solución alternativa para aquellos que no pueden implementar actualizaciones de seguridad de inmediato que consiste en que se **deshabilite SSL-VPN**.

Referencias

- https://www.fortiguard.com/psirt/FG-IR-22-398
- https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/12192-actualizacion-de-seguridad-para-vulnerabilidad-critica-en-fortinet.html

En caso de haber detectado la explotación de esta vulnerabilidad :

debe reportar el incidente mediante correo electrónico a ayudadigital.sspa@juntadeandalucia.es in dicando en el *Asunto: [Compromiso Fortigate1222]*

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