Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM

Boletin de Seguridad UNAM-CERT-2014-008 Dispositivos FortiNet FortiGate y FortiWiFi contienen diversas vulnerabilidades

Una vulnerabilidad que permite un desbordamiento de buffer basado en el heap (heap-based overflow) está presente en los dispositivos FortiGate y FortiWiFi de la marca FortiNet, los cuales además son susceptibles a ataques del tipo "man-in-de-middle" (CWE-300).

- **Fecha de Liberación:** 19-Sep-2014
- **Ultima Revisión:** 25-Sep-2014
- **Fuente:** www.kb.cert.org
- **CVE ID:** VU#730964
- **Riesgo** Moderado
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Ejecución Remota de Código

Sistemas Afectados

FortiGate 4.00.6
FortiWiFi 4.00.6

1. ## Descripción

   Las vulnerabilidades CWE-300 y CWE-122 se encuentran en el servicio FortiManager que utiliza el puerto TCP 541.

   CWE-300: Canal accesible no sólo desde los extremos ('Man-in-the-Middle') - CVE-2014-0351

   El servicio remoto FortiManager depende de certificados SSL del lado del cliente para cifrar el tráfico entre el cliente y el servidor. Es posible para un cliente especificar los métodos de cifrado que se utilizarán para la conexión, incluyendo métodos que no usen certificados para la autenticación, como es el caso de ADH-AES256-SHA. Esto permite que un atacante realice un ataque man-in-the-middle en la comunicación entre el cliente y el servicio FortiManager.

   CWE-122: Desbordamiento de buffer basado en el heap - CVE-2014-2216
   El servicio FortiManager utiliza un protocolo con formato de mensaje que asignará espacio en el heap para ocho apuntadores de parámetros. Sin embargo, cuando se procesa el formato del mensaje, un número arbitrario de apuntadores de parámetros es aceptado. Esto puede causar un desbordamiento de buffer en el heap. Un atacante puede de manera repota ser capaz de explotar esta vulnerabilidad para ejecutar código arbitrario en el dispositivo.
2. ## Impacto

   Al explotar estas vulnerabilidades, un atacante puede conocer de manera no autorizada detalles de la comunicación o ejecutar código arbitrario en los dispositivos.

3. Solución

Fortinet recomienda actualizar FortiOS a las versiones 4.3.16, 5.08 o 5.2.0 para recibir el parche. Además, como medida preventiva se recomienda deshabilitar el servicio de administración remota FortiManager que utiliza el puerto 541.

4. Referencias

- https://cwe.mitre.org/data/definitions/122.html
- https://cwe.mitre.org/data/definitions/300.html
- http://www.fortiguard.com/advisory/FG-IR-14-006/

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47