Boletín de alerta

Boletín Nro.:
Fecha de publicación: 13/05/2025
Tema: Alerta 2025-41 Falla Crítica en Fortinet explotado activamente
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- FortiVoice: versiones 6.4.0–6.4.10, 7.0.0–7.0.6 y 7.2.0.
- FortiMail: versiones hasta la 7.6.2.
- FortiNDR: todas las versiones 1.x y versiones 7.x anteriores a la 7.6.1.
- FortiRecorder: versiones hasta la 7.2.3.
- FortiCamera: versiones hasta la 2.1.3.

Descripción

Se ha revelado una vulnerabilidad crítica de desbordamiento de búfer basada en Stack, identificada como CVE-2025-32756, que afecta a una amplia gama de sus productos de seguridad y red de Fortinet. Con una puntuación CVSS de 9,6, **esta vulnerabilidad permite a atacantes remotos no autenticados ejecutar código o comandos arbitrarios mediante solicitudes HTTP especialmente diseñadas**.

Una vulnerabilidad de desbordamiento basada en Stack [CWE-121] en FortiVoice, FortiMail, FortiNDR, FortiRecorder y FortiCamera podría permitir que un atacante remoto no autenticado ejecute código o comandos arbitrarios mediante solicitudes HTTP diseñadas

Fortinet ha confirmado su explotación activa, especialmente en sistemas FortiVoice.

Indicadores de Compromiso

El proveedor ha proporcionó una lista completa de archivos, procesos y registros asociados con explotaciones conocidas:

Registros Logs

Las siguientes entradas de registro son posibles IOC:

Salida del comando CLI :

diagnose **debug** application httpd display **trace**-log

[x x x x:x:x.x 2025] [fcgid:warn] [pid 1829] [client x.x.x.x:x] mod_fcgid: error reading data, FastCGI server closed connection
[x x x x:x:x.x 2025] [fcgid:error] [pid 1503] mod_fcgid: process /migadmin/www/fcgi/admin.fe(1741) exit(communication error), get unexpected signal 11

Archivos:

Los siguientes archivos del sistema pueden haber sido modificados o añadido:

- [Archivo añadido] /bin/wpad_ac_helper – MD5:4410352e110f82eabc0bf160bec41d21 – archivo principal de malware
- [Archivo añadido] /bin/busybox – MD5:ebce43017d2cb316ea45e08374de7315 y 489821c38f429a21e1ea821f8460e590
- /data/etc/crontab – Se añadió una línea para buscar datos sensibles desde fcgi.debug
- /var/spool/cron/crontabs/root – Se añadió una línea para hacer una copia de seguridad de fcgi.debug

- /var/spool/cron/crontabs/root – Se añadió una línea para hacer una copia de seguridad de fcgi.debug:
- [Archivo añadido] /var/spool/.sync – Las credenciales se recopilan en este archivo mediante los trabajos cron anteriores.
- /etc/pam.d/sshd – Se añadieron líneas Se agregó para incluir libfmlogin.so malicioso
- [Archivo agregado] /lib/libfmlogin.so – MD5:364929c45703a84347064e2d5de45bcd – biblioteca maliciosa que registra el nombre de usuario y la contraseña mediante el inicio de sesión SSH.
- [Archivo agregado] /tmp/.sshdpm – contiene credenciales recopiladas por /lib/libfmlogin.so anterior
- [Archivo agregado] /bin/fmtest – MD5: 2c8834a52faee8d87cff7cd09c4fb946 – Script para escanear la red
- /etc/httpd.conf – Se agregó una línea para incluir calcetines.so: LoadModule calcetines5_module módulos/mod_socks5.so

Mitigación temporal:

Deshabilitar la interfaz administrativa HTTP/HTTPS.

Solución

El proveedor ha lanzado parches de seguridad que corrigen dicha vulnerabilidad y varias versiones y productos:

En la siguiente enlace podrá encontrar información para la actualización de sus dispositivos afectados:

https://docs.fortinet.com/upgrade-tool/fortigate

Información adicional:

- **https://fortiguard.fortinet.com/psirt/FG-IR-25-254**
- https://blog.segu-info.com.ar/2025/05/falla-critica-en-fortinet-explotado.html

- https://nvd.nist.gov/vuln/detail/CVE-2025-32756