# BOLETÍN DE ALERTA

**Boletín Nro.**: 2017-07
**Fecha de publicación**: 25/05/2017
**Tema**: Vulnerabilidad de Ejecución Remota de Código en Samba

**Sistemas afectados**:

- Sambra desde la versión 3.5 hasta 4.6.3, 4.5.9 y 4.4.13

**Descripción**:

Se ha reportado una vulnerabilidad crítica de ejecución remota de código que afecta a Samba, una implementación libre de los protocolos SMB y CIFS, que permite compartir ficheros y otros recursos como impresoras entre sistemas basados en UNIX y sistemas Windows.

La vulnerabilidad que ha sido identificada como CVE-2017-7494, afecta a todas las versiones de Samba de los 7 últimos años, desde la versión 3.5.0 en adelante. La misma permite a un atacante remoto subir una librería compartida a un directorio compartido con permisos de escritura, cargarlo al servidor y ejecutarlo, pudiendo de esta manera ejecutar código remoto arbitrario.

Se han publicado exploits, los cuales pueden ser utilizados fácilmente para la explotación de dicha vulnerabilidad. Actualmente, se han detectado al menos alrededor de 500 IPs con el servicio Samba expuesto hacia Internet.

Samba ha publicado parches para las ramas 4.4.x, 4.5.x y 4.6.x.

**Impacto**

Explotando esta vulnerabilidad un atacante remoto no autorizado podría obtener un control total del servidor que ejecuta la versión vulnerable de Samba.

**Solución**

Samba ha corregido la vulnerabilidad en las versiones 4.6.4, 4.5.10 y 4.4.14.



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py

Sin embargo, no existe parche para las versiones afectadas de la rama 3. Como solución alternativa, en aquellos casos en que no fuera factible la migración a la rama 4, se puede aplicar la siguiente mitigación a través de la adición un parámetro en el fichero *smb.conf* (por lo general, ubicado en /etc/samba/smb.conf) en la sección *[global]*

```
nt pipe support = no
```

Luego de añadir este parámetro, se debe reiniciar el servicio. Esta configuración evita que un atacante pueda abrir una tubería que le permita subir código malicioso a una instalación de Samba; sin embargo, se dejará de compartir recursos con sistemas operativos Windows.

Otra medida de mitigación aplicable a todas las ramas de Samba es evitar la publicación de dicho servicio sobre Internet, en aquellos casos en los que no sea necesaria la compartición de recursos hacia fuera de la red.

**Información adicional:**

https://www.samba.org/samba/security/CVE-2017-7494.html

http://muyseguridad.net/2017/05/25/104-000-samba-ataques-remotos/



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py