SEGURIDAD Y VULNERABILIDADES

Fagor Electronica cuenta con una política de CVD (*Coordinated Vulnerability Disclosure*) establecida que da soporte a aquellos que quieran proporcionar información sobre vulnerabilidades detectadas en sistemas propios de Fagor Electronica.

Es importante resaltar que no es objeto de esta política la notificación de vulnerabilidades observadas, cuando la vulnerabilidad identificada ya tenga un CVE asignado y publicado. En estos supuestos, debe de dirigirse a la sección de reporte de incidentes de Fagor Electronica.

Acciones no permitidas en la búsqueda de vulnerabilidades.

Es muy importante tener en cuenta el respeto a la ley, ya que notificar una vulnerabilidad no implica estar exento de su cumplimiento. Igualmente, buscar vulnerabilidades no puede servir como pretexto para atacar un sistema o cualquier otro objetivo. Varias acciones no están permitidas, por ejemplo:

- Usar ingeniería social
- Comprometer el sistema y mantener el acceso a este de manera persistente.
- Alterar los datos a los que se acceda explotando la vulnerabilidad.
- Utilizar malware.
- Utilizar la vulnerabilidad de cualquier forma más allá de demostrar su existencia. Para demostrar que la vulnerabilidad existe, se pueden usar métodos no agresivos, por ejemplo listando un directorio del sistema.
- Usar fuerza bruta para ganar acceso a los sistemas.
- Compartir la vulnerabilidad con terceros.
- Realizar ataques DoS o DDoS.

En cualquier caso, debe notificarse la vulnerabilidad en cuanto sea detectada y no sacar provecho de ella de forma alguna.

Formulario

ID	CVSS Score	Title	Creation date	Last update