LOTERÍAS Y APUESTAS DEL ESTADO

POLÍTICA SOBRE DIVULGACIÓNES RESPONSABLES

En Sociedad Estatal Loterías y Apuestas del Estado (SELAE) consideramos que la seguridad de nuestros sistemas es una prioridad máxima. Supervisamos y probamos constantemente nuestros sistemas, pero no importa cuánto esfuerzo pongamos en la seguridad del sistema, todavía puede haber vulnerabilidades presentes.

Si encuentra algún indicio de una vulnerabilidad en cualquiera de nuestros sistemas, nos gustaría saber de ella para que podamos tomar medidas para abordarla lo más rápido posible. Esto es para proteger a nuestros usuarios y clientes y evitar que un actor malicioso se aproveche de la situación.

Por favor, siga los siguientes pasos:

- No envíe las vulnerabilidades a través de canales públicos; en su lugar, envíe sus hallazgos por correo electrónico a la dirección incidentes.seginf@selae.es con nuestra clave PGP que tiene como ID 71EF56BB0EC14F00F03B1D38ADEDD6C7F8D360CA.
- No se aproveche de la vulnerabilidad o el problema que haya descubierto, por ejemplo, descargando más datos de los necesarios para demostrar la vulnerabilidad o eliminando o modificando los datos de otras personas.
- No revele el problema a otros hasta que se haya resuelto.
- No realice acciones que puedan tener un impacto en el buen funcionamiento del sistema, tanto en términos de disponibilidad y rendimiento, como en términos de confidencialidad e integridad de los datos
- Proporcione suficiente información (toda la que pueda proporcionar) para ayudarnos a comprender mejor la naturaleza y el alcance del posible problema, de modo que podamos resolverlo lo más rápido posible. Por lo general, la dirección IP o la URL del sistema afectado y una descripción de la vulnerabilidad serán suficientes, pero las vulnerabilidades complejas pueden requerir una explicación más detallada.
- Borre inmediatamente todos los datos obtenidos tan pronto como se informe.
- No solicite compensación por informes de vulnerabilidad de seguridad. SELAE no ofrece actualmente recompensa por errores.

Cómo respondemos:

- Si sigue las pautas anteriores, SELAE considerará su informe de vulnerabilidad y responderemos a su informe dentro de los 7 días hábiles con nuestra evaluación y una fecha de resolución prevista o le solicitaremos más información
- El proceso implica un período de 90 días durante el cual verificamos y reparamos o mitigamos la vulnerabilidad antes de que usted la divulgue a terceros.
- Si se confirma una vulnerabilidad potencial y se determina un riesgo de seguridad significativo, SELAE notificará a sus usuarios y clientes afectados y autoridades de supervisión según corresponda.
- Trataremos su informe con estricta confidencialidad y no comunicaremos sus datos personales a terceros sin su permiso.
- En la información pública sobre el problema informado, lo reconoceremos como el descubridor de la vulnerabilidad, a menos que solicite el anonimato.
- Si ha seguido las instrucciones anteriores, no emprenderemos ninguna acción legal contra usted en relación con el informe.

Nos gustaría agradecerle por ayudarnos a mejorar la seguridad de nuestros sistemas. Realmente apreciamos sus esfuerzos para divulgar el problema de manera responsable.

RESPONSIBLE DISCLOSURE POLICY

At Sociedad Estatal Loterías y Apuestas del Estado (SELAE), we consider the security of our systems a top priority. We supervise and test constantly our systems, but no matter how much effort we put into system security, there can still be vulnerabilities present.

If you find any indication of a vulnerability in any of our systems, we would like to know about it so we can take steps to address it as quickly as possible. The goal is to protect our users and clients and prevent malicious actor from taking advantage of the situation.

Please do the following:

- Do not send the information over public channels; e-mail your findings to incidentes.seginf@selae.es encrypted with our PGP key, that you can also find with ID 71EF56BB0EC14F00F03B1D38ADEDD6C7F8D360CA.
- Do not take advantage of the vulnerability or problem that you have discoverd, for example by downloading more data tan necessary to demonstrate the vulnerability or deleting or modifying other people's data.
- Do not reveal the problem to others until it has been resolved.
- Do not take actions that can affect the operation of the system on its availability or its performance, or can impact confidentiality or integrity of the data.
- Do provide sufficient information (as much as you) can to help us better understand the nature and scope of the possible problem, so that we can resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.
- Do delete all data retrieved once reported.
- Do not demand monetary compensation for the vulnerability report; SELAE does not currently runs a bug bounty program.

How we will respond:

- If you stick to the guidelines above, SLEAE will process your vulnerability report and will respond within 7 business days with our evaluation of the report and expected resolution date or a request for more information.
- Process implies a 90-day period while we verify and repair the vulnerability or mitigate it before you reveal it to third parties
- If the vulnerability is confirmed and poses a significant risk, SELAE will notify affected users and clients and supervising bodies as appropriate.
- Trataremos su informe con estricta confidencialidad y no transmitiremos sus datos personales a terceros sin su permiso.
- In any public communication concerning the reported problem, we will acknowledge you as discoverer unless you oppose.
- If you follow the instructions above, SELAE will not take any legal action against you in relation to your report.

We would like to thank you for helping us improve the security of our systems. We really do appreciate your effort in disclosing the problem in a responsible manner.