# CVE Detail – CVE-2022-42467

When running in prototype mode, the h2 webconsole module (accessible from the Prototype menu) is automatically made available with the ability to directly query the database. It was felt that it is safer to require the developer to explicitly enable this capability. As of 2.0.0-M8, this can now be done using the 'isis.prototyping.h2-console.web-allow-remote-access' configuration property; the web console will be unavailable without setting this configuration. As an additional safeguard, the new 'isis.prototyping.h2-console.generate-random-web-admin-password' configuration parameter (enabled by default) requires that the administrator use a randomly generated password to use the console. The password is printed to the log, as "webAdminPass: xxx" (where "xxx") is the password. To revert to the original behaviour, the administrator would therefore need to set these configuration parameter: isis.prototyping.h2-console.web-allow-remote-access=true isis.prototyping.h2-console.generate-random-web-admin-password=false Note also that the h2 webconsole is never available in production mode, so these safeguards are only to ensure that the webconsole is secured by default also in prototype mode.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.61592

## CVSS Scoring

CVSS v3.1 Score: 5.3

Severity: MEDIUM

## Mapped CWE(s)

* CWE-1188: Initialization of a Resource with an Insecure Default

## CAPEC(s)

* CAPEC-665: Exploitation of Thunderbolt Protection Flaws

## ATT&CK Techniques

* T1542.002: Component Firmware
* T1556: Modify Authentication Process
* T1211: Exploitation for Defense Evasion

## Used By (Actors/Tools)

* Cyclops Blink (malware)
* Kessel (malware)
* Ebury (malware)
* SILENTTRINITY (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Equation (intrusion-set)
* APT28 (intrusion-set)
* FIN13 (intrusion-set)

## Affected Products

* cpe:2.3:a:apache:isis:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apache:isis:2.0.0:milestone1:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apache:isis:2.0.0:milestone2:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apache:isis:2.0.0:milestone3:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apache:isis:2.0.0:milestone4:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apache:isis:2.0.0:milestone5:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apache:isis:2.0.0:milestone6:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apache:isis:2.0.0:milestone7:\*:\*:\*:\*:\*:\*