



CVE-2022-42467

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-42467
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-19 08:15:00 UTC
Updated	2022-10-21 16:43:00 UTC
Description	When running in prototype mode, the h2 webconsole module (accessible from the Prototype menu) is automatically made a

Risk And Classification

Problem Types: CWE-1188

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Isis	All	All	All	All
Application	Apache	Isis	2.0.0	milestone1	All	All
Application	Apache	Isis	2.0.0	milestone2	All	All
Application	Apache	Isis	2.0.0	milestone3	All	All
Application	Apache	Isis	2.0.0	milestone4	All	All
Application	Apache	Isis	2.0.0	milestone5	All	All
Application	Apache	Isis	2.0.0	milestone6	All	All
Application	Apache	Isis	2.0.0	milestone7	All	All

References

Reference
oss-security - ISIS-3128: CVE-2022-42467: Apache Isis: h2 webconsole (available only in prototype mode) should nevertheless be disabled b
lists.apache.org/thread/jbv2ddt00h7ntlbm6vkk4wdmb31pm8q3
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: William Thomson

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)