



CVE-2023-26964

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

Summary

CVE	CVE-2023-26964
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-11 14:15:00 UTC
Updated	2023-11-07 04:09:00 UTC
Description	An issue was discovered in hyper v0.13.7. h2-0.2.4 Stream stacking occurs when the H2 component processes HTTP2 RS

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hyper	H2	0.2.4	All	All	All
Application	Hyper	Hyper	0.13.7	All	All	All

References

Reference

- [SECURITY] Fedora 38 Update: rust-git-delta-0.13.0-5.fc38 - package-announce - Fedora Mailing-Lists
- [SECURITY] Fedora 38 Update: rust-git-delta-0.13.0-5.fc38 - package-announce - Fedora Mailing-Lists
- Stream stacking occurs when H2 processes HTTP2 RST_STREAM frames. As a result, the memory and CPU usage are high. . Issue #2877
- [SECURITY] Fedora 37 Update: rust-bodhi-cli-2.1.0-2.fc37 - package-announce - Fedora Mailing-Lists
- [SECURITY] Fedora 37 Update: rust-bodhi-cli-2.1.0-2.fc37 - package-announce - Fedora Mailing-Lists
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[183964](#) Debian Security Update for rust-h2 (CVE-2023-26964)

[283987](#) Fedora Security Update for clevis (FEDORA-2023-37ae269843)

[284151](#) Fedora Security Update for clevis (FEDORA-2023-cc21019773)

[285317](#) Fedora Security Update for clevis (FEDORA-2023-d88521bfc5)

© [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](#)