



CVE-2022-34970

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

Summary

CVE	CVE-2022-34970
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-04 19:15:00 UTC
Updated	2022-08-10 18:35:00 UTC
Description	Crow before 1.0+4 has a heap-based buffer overflow via the function qs_parse in query_string.h. On successful exploitation

Risk And Classification

Problem Types: CWE-193

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Crowcpp	Crow	All	All	All	All

References

Reference
Release v1.0+4 Security Patch · CrowCpp/Crow · GitHub
Fixed issue where an index in qs_parse is incorrectly incremented beyond the maximum possible value by The-EDev · Pull Request #486 · Cr
CWE - CWE-193: Off-by-one Error (4.7)
CVE-2022-34970/report.md at master · 0xhebi/CVE-2022-34970 · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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