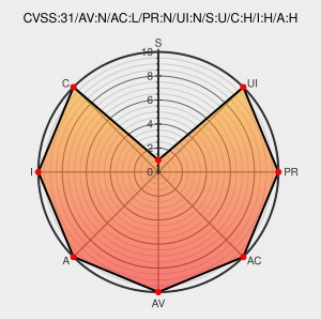
# CVE-2022-38667

Published on: Not Yet Published

Last Modified on: 10/28/2022 07:04:00 PM UTC

## CVE-2022-38667

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Crow from Crowcpp contain the following vulnerability:

HTTP applications (servers) based on Crow through 1.0+4 may allow a Use-After-Free and code execution when HTTP pipelining is used. The HTTP parser supports HTTP pipelining, but the asynchronous Connection layer is unaware of HTTP pipelining. Specifically, the Connection layer is unaware that it has begun processing a later request before it has finished processing an earlier request.

CVE-2022-38667 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

### CVSS3 Score: 9.8 - CRITICAL

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Prevent HTTP pipelining by The-EDev · Pull Request #524 · CrowCpp/Crow · GitHub | github.com text/html | MISC github.com/CrowCpp/Crow/pull/524 |
| CVEs/CVE-2022-38667.md at main · 0xhebi/CVEs · GitHub | github.com text/html | MISC github.com/0xhebi/CVEs/blob/main/Crow/CVE-2022-38667.md |
| CWE - CWE-372: Incomplete Internal State Distinction (4.7) | cwe.mitre.org text/html | MISC cwe.mitre.org/data/definitions/372.html |
| Crow HTTP framework use-after-free - gynvael.coldwind//vx.log | gynvael.coldwind.pl text/html | MISC gynvael.coldwind.pl/?id=753 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:crowcpp:crow:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2022-38667 : HTTP applications servers based on Crow through 1.0+4 may allow a Use-After-Free and code execut… twitter.com/i/web/status/1… | 2022-08-22 20:09:10 |
| @Robo_Alerts | Potentially Critical CVE Detected! CVE-2022-38667 HTTP applications (servers) based on Crow through 1.0+4 may allow… twitter.com/i/web/status/1… | 2022-08-22 20:56:00 |
| @RedPacketSec | Crow code execution \| CVE-2022-38667 - redpacketsecurity.com/crow-code-exec… #CVE #Vulnerability #OSINT #ThreatIntel #Cyber | 2022-08-24 09:02:56 |
| /r/netcve | CVE-2022-38667 | 2022-08-22 21:38:19 |

← Previous ID  Next ID→