Kestrel Denial of Service

Summary

Kestrel of Microsoft ASP.NET Core in .NET 8.0 prior to 8.0.22 and .NET 9.0 prior to 9.0.11 suffers from a remote Denial of Service vulnerability. The vulnerability allows an attacker to cause 100% CPU usage at the server side and paralyze the server. Microsoft Security Response Center privately confirmed and resolved the issue.

Fix commit: 96ccc40

Attack vector

To exploit the vulnerability, an attacker first establishes a benign QUIC connection with the remote Kestrel server. After establishing a successful connection, the attacker sends a QUIC `STREAM` frame with the following parameters.

```
stream_id=6
fin_bit=1
offset=0
payload: empty Qpack Encoder data
```

The vulnerability specifically comes from setting the `finish` bit to `1`.

A single malicious request causes 100% CPU usage on the server. Sending the request continuously (e.g., 1 request every second) causes the server to be unavailable. During this time, a benign client cannot connect to the server.

Releases

No releases published

Packages

No packages published

Contributors 1

IsaJafarov Isa Jafarov