SslHandler doesn't correctly validate packets which can lead to native crash when using native SSLEngine

High **normanmaurer** published **GHSA-4g8c-wm8x-jfhw** yesterday

Package	Affected versions	Patched versions
io.netty:netty-handler (Maven)	4.1.91.Final =< 4.1.117.Final	>= 4.1.118.Final

Description

Impact

When a special crafted packet is received via SslHandler it doesn't correctly handle validation of such a packet in all cases which can lead to a native crash.

Workarounds

As workaround its possible to either disable the usage of the native SSLEngine or changing the code from:

```
SslContext context = ...;
SslHandler handler = context.newHandler(....);
```

to:

```
SslContext context = ...;
SSLEngine engine = context.newEngine(....);
SslHandler handler = new SslHandler(engine, ....);
```

Severity

High 7.5 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2025-24970

Weaknesses

No CWEs

Credits

johnou Reporter