Do not use Wire - Insecure deserialization

Critical rogeralsing published GHSA-hpw7-3vq3-mmv6 on May 11, 2021

Package

Wire (NuGet)

Affected versions

All

Patched versions

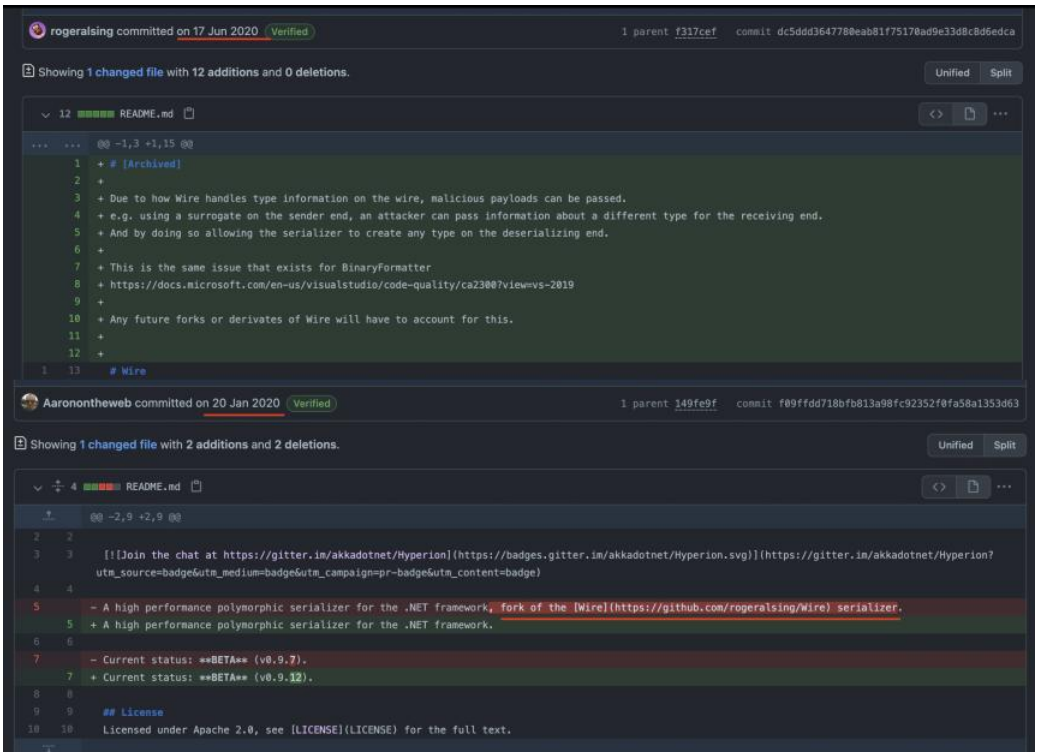
None

Description

Due to how Wire handles type information in its serialization format, malicious payloads can be passed to a deserializer. e.g. using a surrogate on the sender end, an attacker can pass information about a different type for the receiving end. And by doing so allowing the serializer to create any type on the deserializing end.

This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300?view=vs-2019

This also applies to the fork of Wire, AkkaDotNet/Hyperion.
Where we believe the maintainers deliberately are hiding this vulnerability from users:
See how the link to the original repo Wire, as removed from the Hyperion readme, just days after disclosing the vulnerability.



Severity

Critical

CVE ID

CVE-2021-29508

Weaknesses

No CWEs