

Do not use Wire - Insecure deserialization

Critical rogeralsing published GHSA-hpw7-3vq3-mm6 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.

rogeralsing committed on 17 Jun 2020 Verified

1 parent f317cef commit dc5ddd364778@eab81f75178ad9e33d8c8d6dedca

Showing 1 changed file with 12 additions and 0 deletions.

Unified Split

12 README.md

```
... @@ -1,3 +1,15 @@
1 + # [Archived]
2 +
3 + Due to how Wire handles type information on the wire, malicious payloads can be passed.
4 + e.g. using a surrogate on the sender end, an attacker can pass information about a different type for the receiving end.
5 + And by doing so allowing the serializer to create any type on the deserializing end.
6 +
7 + This is the same issue that exists for BinaryFormatter
8 + https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300?view=vs-2019
9 +
10 + Any future forks or derivatives of Wire will have to account for this.
11 +
12 +
13 # Wire
```

Aaronontheweb committed on 20 Jan 2020 Verified

1 parent 149fe9f commit f09ffdd718bfb813a98fc92352f0fa58a1353d63

Showing 1 changed file with 2 additions and 2 deletions.

Unified Split

4 README.md

```
2 2
3 3 [[Join the chat at https://gitter.im/akkadotnet/Hyperion]](https://badges.gitter.im/akkadotnet/Hyperion.svg)](https://gitter.im/akkadotnet/Hyperion?
4 4 utm_source=badge&utm_medium=badge&utm_campaign=pr-badge&utm_content=badge)
5 - A high performance polymorphic serializer for the .NET framework, fork of the [Wire](https://github.com/rogeralsing/Wire) serializer.
6 + A high performance polymorphic serializer for the .NET framework.
7 - Current status: **BETA** (v0.9.7).
8 + Current status: **BETA** (v0.9.12).
9
10 ## License
11 Licensed under Apache 2.0, see [LICENSE](LICENSE) for the full text.
```

Severity

Critical

CVE ID

CVE-2021-29508

Weaknesses

No CWEs