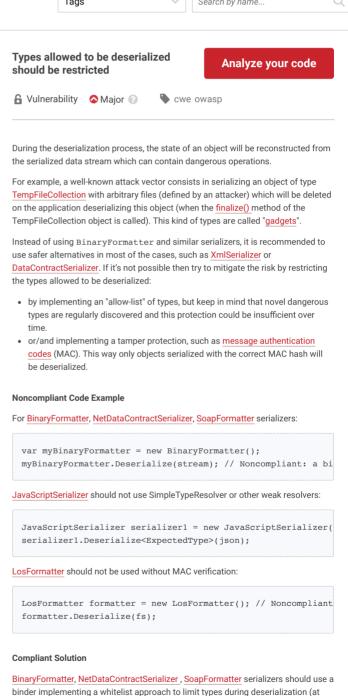


used



least one exception should be thrown or a null value returned):

sealed class CustomBinder : SerializationBinder

public override Type BindToType(string assemblyName, stri

if (!(typeName == "type1" || typeName == "type2" || t

Code Smell

Exceptions should not be thrown from property getters

Code Smell

Unused type parameters should be removed

Code Smell

Parameters should be passed in the correct order

Code Smell

Two branches in a conditional structure should not have exactly the

```
throw new SerializationException("Only type1, type
       return Assembly.Load(assemblyName).GetType(typeName);
  }
}
var myBinaryFormatter = new BinaryFormatter();
myBinaryFormatter.Binder = new CustomBinder();
myBinaryFormatter.Deserialize(stream);
```

JavaScriptSerializer should use a resolver implementing a whitelist to limit types during deserialization (at least one exception should be thrown or a null value returned):

```
public class CustomSafeTypeResolver : JavaScriptTypeResolver
   public override Type ResolveType(string id)
      if(id != "ExpectedType") {
        throw new ArgumentNullException("Only ExpectedType
      return Type.GetType(id);
JavaScriptSerializer serializer = new JavaScriptSerializer(n
serializer.Deserialize<ExpectedType>(json);
```

LosFormatter serializer with MAC verification:

```
LosFormatter formatter = new LosFormatter(true, secret); //
formatter.Deserialize(fs);
```

- OWASP Top 10 2021 Category A8 Software and Data Integrity Failures
- docs.microsoft.com BinaryFormatter security guide
- OWASP Top 10 2017 Category A8 Insecure Deserialization
- MITRE, CWE-134 Use of Externally-Controlled Format String
- MITRE, CWE-502 Deserialization of Untrusted Data
- SANS Top 25 Risky Resource Management
- OWASP Deserialization Cheat Sheet

Available In:

sonarlint ⊚ | sonarcloud ♦ | sonarqube

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved. Privacy Policy