Deserialization of Untrusted Data

Affecting singoocms.utility package, versions **[0,]**

Snyk CVSS

Exploit Maturity	**Proof of concept**
Attack Complexity	**High**
Integrity	HIGH
Availability	HIGH

See more

INTRODUCED: 8 DEC 2021 CVE-2022-0749
CWE-502 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `SinGooCMS.Utility`.

Overview

SinGooCMS.Utility is a collection of tools, including configuration, file, date, data, serialization, reflection, image processing, network, cache, Web related, encryption and decryption, compression, class expansion and other tools, almost covering the development of All tool requirements! Support netstandard2.1 and net framework 4.6.1.

Affected versions of this package are vulnerable to Deserialization of Untrusted Data. The socket client in the package can pass in the payload via the user-controllable input after it has been established, because this socket client transmission does not have the appropriate restrictions or type bindings for the `BinaryFormatter`.

Details

Serialization is a process of converting an object into a sequence of bytes which can be persisted to a disk or database or can be sent through streams. The reverse process of creating object from sequence of bytes is called deserialization. Serialization is commonly used for communication (sharing objects between multiple hosts) and

NVD 9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and

persistence (store the object state in a file or a database). It is an integral part of popular protocols like *Remote Method Invocation (RMI)*, *Java Management Extension (JMX)*, *Java Messaging System (JMS)*, *Action Message Format (AMF)*, *Java Server Faces (JSF) ViewState*, etc.

Deserialization of untrusted data (CWE-502) is when the application deserializes untrusted data without sufficiently verifying that the resulting data will be valid, thus allowing the attacker to control the state or the flow of the execution.

References

- GitHub Issue
- Vulnerable Code

in your application, and suggest you quick fixes.

Test your applications

Snyk ID	**SNYK-DOTNET-SINGOOCMSUTILITY-2312979**
Published	**27 Feb 2022**
Disclosed	**8 Dec 2021**
Credit	**Keyang Yin, zpbrent(zhou, peng@shu)**

Report a new vulnerability

Found a mistake?

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon

Join the >> community

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.