



CVE-2018-1000210

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-1000210
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-13 18:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	YamlDotNet version 4.3.2 and earlier contains a Insecure Direct Object Reference vulnerability in The default behavior of D

Risk And Classification

Problem Types: CWE-502 | CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yamldotnet Project	Yamldotnet	All	All	All	All

References

Reference	Source
YamlDotNet/TypeNameInTagNodeTypeResolver.cs at f96b7cc40a0498f8bafdeb49df3aa23aa2c60993 · aaubry/YamlDotNet · GitHub	CONF
aaubry/YamlDotNet · GitHub	CONF
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980876](#) Dotnet (nuget) Security Update for YamlDotNet.Signed (GHSA-rpch-cqj9-h65r)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report