



CVE-2020-8867

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

Summary

CVE	CVE-2020-8867
State	PUBLIC
Assigner	zdi-disclosures@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-22 21:15:00 UTC
Updated	2020-04-29 14:45:00 UTC
Description	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of OPC Foundation

Risk And Classification

Problem Types: CWE-613

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opcfoundation	Unified Architecture .net-standard	All	All	All	All

References

Reference	Source	Link	Tags
ZDI-20-536 Zero Day Initiative	MISC	www.zerodayinitiative.com	Third
opcfoundation.org/SecurityBulletins/OPC%20Foundation%20Security%20Bulletin%20CV...	MISC	opcfoundation.org	Vend
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981817 Dotnet (nuget) Security Update for OPCFoundation.NetStandard.Opc.Ua (GHSA-9q94-v7ch-mxqw)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)