CVE-2018-0785

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-0785
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-10 01:29:00 UTC
Updated	2018-02-01 21:09:00 UTC
Description	ASP.NET Core 1.0. 1.1, and 2.0 allow a cross site request forgery vulnerability due to the ASP.NET Core project templates

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Asp.net Core	2.0	All	All	All
Application	Microsoft	Asp.net Core	2.0	All	All	All

References

Reference
ASP.NET Input Validation Flaws Let Remote Users Conduct Cross-Site Request Forgery and Cross-Site Scripting Attacks - SecurityTracker
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0785
Microsoft ASP.NET Core CVE-2018-0785 Cross Site Request Forgery Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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