CVE-2018-0787

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

Summary

CVE	CVE-2018-0787
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-14 17:29:00 UTC
Updated	2018-04-11 15:07:00 UTC
Description	ASP.NET Core 1.0. 1.1, and 2.0 allow an elevation of privilege vulnerability due to how web applications that are created fr

Risk And Classification

Problem Types: CWE-640

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Asp.net Core	1.0	All	All	All
Application	Microsoft	Asp.net Core	1.1	All	All	All
Application	Microsoft	Asp.net Core	2.0	All	All	All
Application	Microsoft	Asp.net Core	1.0	All	All	All
Application	Microsoft	Asp.net Core	1.1	All	All	All
Application	Microsoft	Asp.net Core	2.0	All	All	All

References

Reference
ASP.NET Kestrel Web Application HTML Injection Flaw Lets Remote Users Reset the Target User's Password - SecurityTracker
Microsoft Security Advisory CVE-2018-0787: ASP.NET Core Elevation Of Privilege Vulnerability · Issue #295 · aspnet/Announcements · GitHu
Microsoft ASP.NET Core CVE-2018-0787 Remote Privilege Escalation Vulnerability
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0787
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981395 Dotnet (nuget) Security Update for Microsoft.AspNetCore.Server.Kestrel.Core (GHSA-365p-96qv-xr7g)