CVE-2018-0875

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

Summary

CVE	CVE-2018-0875
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-14 17:29:00 UTC
Updated	2021-08-12 17:19:00 UTC
Description	.NET Core 1.0, .NET Core 1.1, NET Core 2.0 and PowerShell Core 6.0.0 allow a denial of Service vulnerability due to how

Risk And Classification

Problem Types: NVD-CWE-noinfo

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
Application	Microsoft	Powershell Core	6.0	All	All	All
Application	Microsoft	Powershell Core	6.0.0	All	All	All
Application	Microsoft	Powershell Core	6.0.0	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Pa
Microsoft .NET CVE-2018-0875 Denial Of Service Vulnerability	BID	www.securityfocus.com	Third Pa
Microsoft .NET Hash Collision Bug Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.com	Third Pa
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0875	CONFIRM	portal.msrc.microsoft.com	Patch, V
CVE Program record	CVE.ORG	www.cve.org	canonica

NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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**