CVE-2017-0016

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

Summary

CVE	CVE-2017-0016
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-17 00:59:00 UTC
Updated	2017-07-25 01:29:00 UTC
Description	Microsoft Windows 10 Gold, 1511, and 1607; Windows 8.1; Windows RT 8.1; Windows Server 2012 R2, and Windows Serv

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Operating System	Microsoft	Windows Rt 8.1	All	All	All	All
Operating System	Microsoft	Windows Rt 8.1	All	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	All	All	All	All
Operating System	Microsoft	Windows Server 2016	All	All	All	All

References

Reference

Microsoft Windows CVE-2017-0016 Memory Corruption Vulnerability
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0016
Microsoft Windows Server Message Block SMBv3 Response Processing Bug Lets Remote Users Cause the Target System to Crash - Securit
Microsoft Windows Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information, Deny Service, and Execute Arbitrary Code and
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**