CVE-2020-0796

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

Summary

CVE	CVE-2020-0796
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-12 16:15:00 UTC
Updated	2022-04-22 19:02:00 UTC
Description	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol ha

Risk And Classification

EPSS: 0.944080000 probability, percentile 0.999780000 (date 2026-04-08)

CISA KEV: Listed on 2022-02-10; due 2022-08-10; ransomware use Known

Problem Types: CWE-119

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	SMBv3
Name	Microsoft SMBv3 Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-0796

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All

References

Reference	Source	Link
SMBleed / SMBGhost Pre-Authentication Remote Code Execution Proof Of Concept ≈ Packet Storm	MISC	packetstormsecurity.com
SMBv3 Compression Buffer Overflow ≈ Packet Storm	MISC	packetstormsecurity.com
Microsoft Windows SMBGhost Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com
Microsoft Windows 10 SMB 3.1.1 Local Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com
Microsoft Windows SMB 3.1.1 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796	MISC	portal.msrc.microsoft.com
CoronaBlue / SMBGhost Microsoft Windows 10 SMB 3.1.1 Proof Of Concept ≈ Packet Storm	MISC	packetstormsecurity.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

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