CVE-2017-0148

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

Summary

CVE	CVE-2017-0148
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-17 00:59:04 UTC
Updated	2026-04-22 13:50:29 UTC
Description	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.940670000 probability, percentile 0.999050000 (date 2026-04-22)

CISA KEV: Listed on 2022-04-06; due 2022-04-27; ransomware use Known

Problem Types: CWE-20 | Remote Code Execution | CWE-20 CWE-20 Improper Input Validation

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9.3		AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	SMBv1 server
Name	Microsoft SMBv1 Server Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-0148

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Server Message Block	1.0	All	All	All
Operating System	Microsoft	Windows 10 1507	-	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 7	-	sp1	All	All

Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Hardware	Siemens	Acuson P300	-	All	All	All
Operating System	Siemens	Acuson P300 Firmware	13.02	All	All	All
Operating System	Siemens	Acuson P300 Firmware	13.03	All	All	All
Operating System	Siemens	Acuson P300 Firmware	13.20	All	All	All
Operating System	Siemens	Acuson P300 Firmware	13.21	All	All	All
Hardware	Siemens	Acuson P500	-	All	All	All
Operating System	Siemens	Acuson P500 Firmware	va10	All	All	All
Operating System	Siemens	Acuson P500 Firmware	vb10	All	All	All
Hardware	Siemens	Acuson Sc2000	-	All	All	All
Operating System	Siemens	Acuson Sc2000 Firmware	All	All	All	All
Operating System	Siemens	Acuson Sc2000 Firmware	5.0a	All	All	All
Hardware	Siemens	Acuson X700	-	All	All	All
Operating System	Siemens	Acuson X700 Firmware	1.0	All	All	All
Operating System	Siemens	Acuson X700 Firmware	1.1	All	All	All
Hardware	Siemens	Syngo Sc2000	-	All	All	All
Operating System	Siemens	Syngo Sc2000 Firmware	5.0a	All	All	All
Operating System	Siemens	Syngo Sc2000 Firmware	All	All	All	All
Hardware	Siemens	Tissue Preparation System	-	All	All	All
Operating System	Siemens	Tissue Preparation System Firmware	All	All	All	All
Hardware	Siemens	Versant Kpcr Molecular System	-	All	All	All
Operating System	Siemens	Versant Kpcr Molecular System Firmware	All	All	All	All
Hardware	Siemens	Versant Kpcr Sample Prep	-	All	All	All
Operating System	Siemens	Versant Kpcr Sample Prep Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Microsoft Corporation	Windows SMB	affected The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 a

References

Reference
Windows Server Message Block Request Handling Flaws Let Remote Users Obtain Potentially Sensitive Information and Execute Arbitrary Co
cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf
Philips Intellispace Portal ISP Vulnerabilities | ICS-CERT
{{windowTitle}}
SMB DOUBLEPULSAR Remote Code Execution ≈ Packet Storm
www.cisa.gov/known-exploited-vulnerabilities-catalog
Exploit – Page 41891 – Exploits Database
DOUBLEPULSAR Payload Execution / Neutralization ≈ Packet Storm
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)
Microsoft Windows SMB Server CVE-2017-0148 Remote Code Execution Vulnerability
cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-04-06T00:00:00.000Z	CVE-2017-0148 added to CISA KEV

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