



# CVE-2017-0147

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2017-0147  |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | microsoft  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2017-03-17 00:59:04 UTC  |
| <b>Updated</b>         | 2026-04-22 13:50:27 UTC  |
| <b>Description</b>     | 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 7.5 HIGH from nvd@nist.gov

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

**EPSS:** 0.924180000 probability, percentile 0.997320000 (date 2026-04-22)

**CISA KEV:** Listed on 2022-05-24; due 2022-06-14; ransomware use Known

**Problem Types:** NVD-CWE-noinfo | Information Disclosure | CWE-noinfo Not enough information

| Version | Source                               | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------------|-----------|-------|----------|--|
| 3.1     | nvd@nist.gov                         | Primary   | 7.5   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |
| 3.1     | ADP                                  | DECLARED  | 7.5   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |
| 3.1     | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 7.5   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |
| 2.0     | nvd@nist.gov                         | Primary   | 4.3   |          | AV:N/AC:M/Au:N/C:P/I:N/A:N                   |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

### CISA Known Exploited Vulnerability

|                        |   |
|------------------------|---|
| <b>Vendor</b>          | Microsoft   |
| <b>Product</b>         | SMBv1 server  |
| <b>Name</b>            | Microsoft Windows SMBv1 Information Disclosure Vulnerability  |
| <b>Required Action</b> | Apply updates per vendor instructions.  |
| <b>Notes</b>           | <a href="https://nvd.nist.gov/vuln/detail/CVE-2017-0147">https://nvd.nist.gov/vuln/detail/CVE-2017-0147</a> |

### NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor    | Product         | Version | Update | Edition | Language |
|------------------|-----------|-----------------|---------|--------|---------|----------|
| 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                  | All   | All | All | All |
| Operating System | Siemens   | Syngo Sc2000 Firmware                  | 5.0a  | 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

[www.cisa.gov/known-exploited-vulnerabilities-catalog](http://www.cisa.gov/known-exploited-vulnerabilities-catalog)

[cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf](http://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf)

Philips Intellispace Portal ISP Vulnerabilities | ICS-CERT

SMB DOUBLEPULSAR Remote Code Execution ≈ Packet Storm

Exploit – Page 41891 – Exploits Database

DOUBLEPULSAR Payload Execution / Neutralization ≈ Packet Storm

Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010) - Windows

Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)

Microsoft Windows SMB Server CVE-2017-0147 Information Disclosure Vulnerability

[cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf](http://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf)

{{windowTitle}}

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    | 2022-05-24T00:00:00.000Z | CVE-2017-0147 added to CISA KEV |

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)