



CVE-2017-8584

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

Summary

CVE	CVE-2017-8584
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-11 21:29:01 UTC
Updated	2025-04-20 01:37:25 UTC
Description	Windows 10 1607 and Windows Server 2016 allow an attacker to execute code remotely via a specially crafted WiFi packet

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Problem Types: NVD-CWE-noinfo | Remote Code Execution

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.9		AV:A/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows Server 2016	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft Corporation	Windows 10 1607 And Windows Server 2016	affected Microsoft Windows	Not specified

References

Reference	Source
{{windowTitle}}	af854c
Microsoft HoloLens WiFi Packet Processing Bug Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker	af854c
Microsoft Windows Hololens CVE-2017-8584 Remote Code Execution Vulnerability	af854c
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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

CVE.report and Source URL Uptime Status [status.cve.report](#)