CVE-2016-3274

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

Summary

CVE	CVE-2016-3274
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-13 01:59:29 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to conduct content-spoofing attacks via

Risk And Classification

Primary CVSS: v3.0 3.1 LOW from nvd@nist.gov

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

Problem Types: CWE-284 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	3.1	LOW	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N
2.0	nvd@nist.gov	Primary	2.6		AV:N/AC:H/Au:N/C:N/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Edge	All	All	All	All
Application	Microsoft	Internet Explorer	10	All	All	All
Application	Microsoft	Internet Explorer	11	All	All	All
Application	Microsoft	Internet Explorer	9	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Microsoft Security Bulletin MS16-084 - Critical | Microsoft Docs
Microsoft Internet Explorer Multiple Bugs Let Remote Users Spoof Web Content, Bypass Security Restrictions, Conduct Cross-Site Scripting A
Malformed Request
Microsoft Security Bulletin MS16-085 - Critical | Microsoft Docs
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**