



CVE-2016-3351

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

Summary

CVE	CVE-2016-3351
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-14 10:59:24 UTC
Updated	2026-04-22 16:43:06 UTC
Description	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a cra

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.454070000 probability, percentile 0.976510000 (date 2026-05-17)

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

Problem Types: NVD-CWE-noinfo | n/a | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	2.6		AV:N/AC:H/Au:N/C:P/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Internet Explorer and Edge
Name	Microsoft Internet Explorer and Edge Information Disclosure Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2016-3351

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Edge	-	All	All	All
Application	Microsoft	Internet Explorer	10	All	All	All
Application	Microsoft	Internet Explorer	11	-	All	All
Application	Microsoft	Internet Explorer	9	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 Vista	-	sp2	All	All

Vendor Declared Affected Products

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

References

Reference
Microsoft Edge Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information and Execute Arbitrary Code - SecurityTracker
Detecting analysts before installing the malware – Broken Browser
www.cisa.gov/known-exploited-vulnerabilities-catalog
Microsoft Security Bulletin MS16-104 - Critical Microsoft Docs
Microsoft Internet Explorer Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information, Bypass Security, Execute Arbitrary Code
Microsoft Security Bulletin MS16-105 - Critical Microsoft Docs
Microsoft Internet Explorer and Edge CVE-2016-3351 Information Disclosure Vulnerability
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-2016-3351 added to CISA KEV

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

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