CVE-2015-1635

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

Summary

CVE	CVE-2015-1635
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-14 20:59:01 UTC
Updated	2026-04-22 16:42:38 UTC
Description	HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 201

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from ADP

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

EPSS: 0.943100000 probability, percentile 0.999480000 (date 2026-04-25)

CISA KEV: Listed on 2022-02-10; due 2022-08-10; ransomware use Unknown

Problem Types: CWE-94 | n/a | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	HTTP.sys
Name	Microsoft HTTP.sys Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2015-1635

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	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

Vendor Declared Affected Products

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

References

Reference	Source
Microsoft Security Bulletin MS15-034 - Critical | Microsoft Docs	af854a3a-2127-422
Microsoft Windows HTTP Protocol Stack CVE-2015-1635 Remote Code Execution Vulnerability	af854a3a-2127-422
www.osvdb.org/120629	af854a3a-2127-422
Windows HTTP Protocol Stack ('HTTP.sys') Parsing Error Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2
MS Windows HTTP.sys - HTTP Request Parsing DoS MS15-034	af854a3a-2127-422
Microsoft Window - HTTP.sys PoC MS15-034	af854a3a-2127-422
Microsoft Windows HTTP.sys Proof Of Concept ≈ Packet Storm	af854a3a-2127-422
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-02-10T00:00:00.000Z	CVE-2015-1635 added to CISA KEV

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