CVE-2017-0199

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

Summary

CVE	CVE-2017-0199
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-12 14:59:01 UTC
Updated	2026-04-22 13:50:36 UTC
Description	Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Window

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

EPSS: 0.943020000 probability, percentile 0.999460000 (date 2026-04-21)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Known

Problem Types: NVD-CWE-noinfo | Remote Code Execution | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9.3		AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Office and WordPad
Name	Microsoft Office and WordPad Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-0199

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office	2007	sp3	All	All
Application	Microsoft	Office	2010	sp2	All	All
Application	Microsoft	Office	2013	sp1	All	All
Application	Microsoft	Office	2016	-	All	All
Operating System	Microsoft	Windows 7	-	sp1	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 Vista	-	sp2	All	All
Application	Philips	Intellispace Portal	7.0	All	All	All
Application	Philips	Intellispace Portal	8.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Microsoft Corporation	Office/WordPad	affected Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsc

References

Reference
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199
Philips Intellispace Portal ISP Vulnerabilities | ICS-CERT
CVE-2017-0199 Practical exploitation ! (PoC)
Microsoft Office Word - '.RTF' Malicious HTA Execution (Metasploit)
Microsoft Office File OLE-Based Processing Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker
www.cisa.gov/known-exploited-vulnerabilities-catalog
Exploit – Page 41894 – Exploits Database
Analysis of a CVE-2017-0199 Malicious RTF Document | NVISO LABS – blog
Microsoft Office OLE Feature Remote Code Execution Vulnerability
CVE-2017-0199 Used as Zero Day to Distribute FINSPY Espionage Malware and LATENTBOT Cyber Crime Malware « CVE-2017-0199 Usec
Exploiting CVE-2017-0199: HTA Handler Vulnerability – MDSec
Microsoft Excel - OLE Arbitrary Code Execution
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	2021-11-03T00:00:00.000Z	CVE-2017-0199 added to CISA KEV

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