CVE-2017-11882

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

Summary

CVE	CVE-2017-11882
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-15 03:29:01 UTC
Updated	2026-04-22 13:48:45 UTC
Description	Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Mic

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: 0.943540000 probability, percentile 0.999610000 (date 2026-05-12)

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

Problem Types: CWE-119 | Remote Code Execution | CWE-119 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

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
Name	Microsoft Office Memory Corruption Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-11882

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	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Microsoft Corporation	Microsoft Office	affected Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Mic

References

Reference
Microsoft Office - OLE Remote Code Execution - Windows remote Exploit
GitHub - rxwx/CVE-2017-11882: Proof-of-Concept exploits for CVE-2017-11882
Microsoft Excel Bugs Let Remote Users Bypass Security and Execute Arbitrary Code - SecurityTracker
Microsoft Office CVE-2017-11882 Memory Corruption Vulnerability
GitHub - 0x09AL/CVE-2017-11882-metasploit: This is a Metasploit module which exploits CVE-2017-11882 using the POC released here : htt
GitHub - embedi/CVE-2017-11882: Proof-of-Concept exploits for CVE-2017-11882
0patch Blog: Did Microsoft Just Manually Patch Their Equation Editor Executable? Why Yes, Yes They Did. (CVE-2017-11882)
Fileless Code Injection in Word without macros (CVE-2017-11882) « reversingminds's Blog
GitHub - unamer/CVE-2017-11882: CVE-2017-11882 Exploit accepts over 17k bytes long command/code in maximum.
Skeleton in the closet. MS Office vulnerability you didn't know about – Embedi
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882
Analysis of CVE-2017-11882 Exploit in the Wild - Palo Alto Networks Blog
www.cisa.gov/known-exploited-vulnerabilities-catalog
Vulnerability Note VU#421280 - Microsoft Office Equation Editor stack buffer overflow
0patch Blog: Microsoft's Manual Binary Patch For CVE-2017-11882 Meets 0patch
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-2017-11882 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