CVE-2017-11774

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

Summary

CVE	CVE-2017-11774
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-13 13:29:00 UTC
Updated	2026-04-22 13:48:34 UTC
Description	Microsoft Outlook 2010 SP2, Outlook 2013 SP1 and RT SP1, and Outlook 2016 allow an attacker to execute arbitrary comr

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: 0.855700000 probability, percentile 0.993760000 (date 2026-05-02)

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

Problem Types: CWE-119 | Security Feature Bypass | 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	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

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

Partial

Integrity

Partial

Availability

Partial

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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Office
Name	Microsoft Office Outlook Security Feature Bypass Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-11774

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Outlook	2010	sp2	All	All
Application	Microsoft	Outlook	2013	sp1	All	All
Application	Microsoft	Outlook	2013	sp1	All	All
Application	Microsoft	Outlook	2016	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft Corporation	Microsoft Outlook	affected Microsoft Outlook 2010 SP2	Not specified
CNA	Microsoft Corporation	Microsoft Outlook	affected Outlook 2013 SP1 and RT SP1	Not specified
CNA	Microsoft Corporation	Microsoft Outlook	affected Outlook 2016	Not specified

References

Reference
www.cisa.gov/known-exploited-vulnerabilities-catalog
Microsoft Outlook Security Flaws Let Remote Users Bypass Security to Execute Arbitrary Commands and Obtain User Email Content - Securi
SensePost | Outlook home page – another ruler vector
{{windowTitle}}
Microsoft Office Outlook CVE-2017-11774 Security Bypass 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	2021-11-03T00:00:00.000Z	CVE-2017-11774 added to CISA KEV

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