

CVE-2021-23874

McAfee Total Protection (MTP) Improper Privilege Management Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Arbitrary Process Execution vulnerability in McAfee Total Protection (MTP) prior to 16.0.30 allows a local user to gain elevated privileges and execute arbitrary code bypassing MTP self-defense.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.010 63.3rd percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · listed over a year
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.010 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
total protection	< 16.0.30	16.0.30	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-jx9f-q7vh-wf4p	NVD	nvd.nist.gov/vuln/detail/CVE-2021-23874
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-10800
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-23874		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.