

CVE-2023-41179

Trend Micro Apex One and Worry-Free Business Security Remote Code Execution Vulnerability

CISA KEV since Sep 21, 2023

Actively exploited

A vulnerability in the 3rd party AV uninstaller module contained in Trend Micro Apex One (on-prem and SaaS), Worry-Free Business Security and Worry-Free Business Security Services could allow an attacker to manipulate the module to execute arbitrary commands on an affected installation. Note that an attacker must first obtain administrative console access on the target system in order to exploit this vulnerability.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.2 High · NVD	EPSS 0.043 91st percentile · FIRST	CISA DEADLINE Oct 12, 2023 KEV since 2023 · 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	0.043 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
apex one	2019	no fixed version listed	NVD
worry-free business security	10.0	no fixed version listed	NVD
worry-free business security services	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-vq2c-8m6j-g4vh	success.trendmicro.com	success.trendmicro.com/dcx/s/solution/000294994?language=en_US
NVD	nvd.nist.gov/vuln/detail/CVE-2023-41179	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-45696	Current data	evulnable.com/vulnerability-management/cve/CVE-2023-41179

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