

CVE-2019-4716

IBM Planning Analytics Remote Code Execution Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

IBM Planning Analytics 2.0.0 through 2.0.8 is vulnerable to a configuration overwrite that allows an unauthenticated user to login as "admin", and then execute code as root or SYSTEM via TM1 scripting. IBM X-Force ID: 172094.

EVRS 83 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.864 99.74th percentile · FIRST	CISA DEADLINE May 3, 2022 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	0.864 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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
planning analytics	≥ 2.0 ≤ 2.0.8	after 2.0.8	NVD

Sources

Vendor guidance ibm.com/support/pages/node/1127781**Additional guidance** exchange.xforce.ibmcloud.com/vulnerabilities/172094**NVD** nvd.nist.gov/vuln/detail/CVE-2019-4716**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2019-14323**Current data** evulnable.com/vulnerability-management/cve/CVE-2019-4716

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