

CVE-2020-15505

Ivanti MobileIron Multiple Products Remote Code Execution Vulnerability

Exigent
CISA KEV since Nov 3, 2021
Actively exploited
Public exploit module (Metasploit)

A remote code execution vulnerability in MobileIron Core & Connector versions 10.3.0.3 and earlier, 10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4.0.3, 10.5.1.0, 10.5.2.0 and 10.6.0.0; and Sentry versions 9.7.2 and earlier, and 9.8.0; and Monitor and Reporting Database (RDB) version 2.0.0.1 and earlier that allows remote attackers to execute arbitrary code via unspecified vectors.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.997 99.95th 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	0.997 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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
core	< 10.3.0.4 ≥ 10.4.0.0 < 10.4.0.4 ≥ 10.5.1.0 < 10.5.1.1 ≥ 10.5.2.0 < 10.5.2.1 ≥ 10.6.0.0 < 10.6.0.1	10.3.0.4 · 10.4.0.4 · 10.5.1.1 · 10.5.2.1 · 10.6.0.1	NVD
enterprise connector	< 10.3.0.4 ≥ 10.4.0.0 < 10.4.0.4 ≥ 10.5.1.0 < 10.5.1.1 ≥ 10.5.2.0 < 10.5.2.1 ≥ 10.6.0.0 < 10.6.0.1	10.3.0.4	NVD
monitor and reporting database	< 2.0.0.2	no fixed version listed	NVD
sentry	≥ 9.7.0 < 9.7.3 ≥ 9.8.0 < 9.8.1	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-779w-wqpf-gq64	Additional guidance	mobileiron.com/en/blog/mobileiron-security-updates-available
NVD	nvd.nist.gov/vuln/detail/CVE-2020-15505	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-7497	Current data	evulnable.com/vulnerability-management/cve/CVE-2020-15505

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