

Forum:[Hack Forums](#)

Thread: [One threat actor responsible for 83% of recent Ivanti RCE attacks](#)

MadScientist - February 15, 2026, 2:31 pm

Threat intelligence observations show that a single threat actor is responsible for most of the active exploitation of two critical vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM), tracked as CVE-2026-1281 and CVE-2026-1340.

The security issues have been flagged as actively exploited in zero-day attacks in Ivanti's security advisory, where the company also announced hotfixes

Both flaws received a critical severity rating and allow an attacker to inject code without authentication, leading to remote code execution (RCE) on vulnerable systems.

A single IP address hosted on bulletproof infrastructure is responsible for over 83% of exploitation activity related to the two vulnerabilities, says threat-focused internet intelligence company GreyNoise.

Between February 1st and 9th, the monitoring platform observed 417 exploitation sessions originating from 8 unique source IP addresses, and centered on CVE-2026-1281 and CVE-2026-1340.

The highest volume, 83%, comes from 193[.]24[.]123[.]42, hosted by PROSPERO OOO (AS200593), which Censys analysts marked as a bulletproof autonomous system used to target various software products

Source -

<https://www.bleepingcomputer.com/news/security/one-threat-actor-responsible-for-83-percent-of-recent-ivanti-rce-attacks/>