CYBER ADVISORY

Thursday, January 29, 2026

CSIC-ADVISORY-202601-A-010

Code Injection Vulnerabilites in Ivanti Endpoint Manager Mobile (EPMM)

Remote Code Execution	Data Exfiltration	Exploited in the Wild	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has identified two critical vulnerabilities impacting Ivanti's Endpoint Manager Mobile. CVE-2026-1281 carries a CVSS 3.1 score of 9.8, and CVE-2026-1340 which carries a CVSS 3.1 score of 9.8.[1][2] Successful exploitation of these vulnerabilities could lead to unauthenticated remote code execution. The attacker would be able to execute arbitrary shell commands, install persistent backdoors, or exfiltrate data.

CVE-2026-1281 and CVE-1340 have both been confirmed to be exploited in the wild. The vendor has issued a security advisory with patching and workaround instructions.

The Cal-CSIC recommends immediately following the vendor's guidance in mitigation and remediation, to include immediate patching. If patching is not immediately feasible, please follow the vendor's instructions for a workaround.[3]

For further information on Ivanti's security advisory and analysis please use these links:

Security Advisory

https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US

Vendor Analysis

https://forums.ivanti.com/s/article/Analysis-Guidance-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US

Affected Product:

Product Name	Affected Version(s)	Resolved Version(s)
Ivanti Endpoint Manager Mobile	12.5.0.0 and prior 12.6.0.0 and prior 12.7.0.0 and prior	RPM 12.x.0.x
	12.5.1.0 and prior 12.6.1.0 and prior	RPM 12.x.1.x
Customers should apply either RPM 12.x.0.x or RPM 12.x.1.x, depending on their version. Customers do not need to apply both RPMs as they are version-specific, not vulnerability specific. [4]		

References

[1] CVE.org; "CVE-2026-1281"; https://www.cve.org/CVERecord?id=CVE-2026-1340/; accessed 29 January 2026
[2] CVE.org; "CVE-2026-1340"; https://www.cve.org/CVERecord?id=CVE-2026-1281/ accessed 29 January 2026
[3] Ivanti; "Security Advisory Ivanti Endpoint Manager Mobile (EPMM) (CVE2026-1281 &CVE-2026-1340)"; https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US; accessed 29 January 2026
[4] Ivanti; "Security Advisory Ivanti Endpoint Manager Mobile (EPMM) (CVE2026-1281 &CVE-2026-1340)"; https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US; accessed 29 January 2026