ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

NOTE DE SECURITE

Titre	Vulnérabilités critiques activement exploitées affectant Ivanti Endpoint Manager Mobile
Numéro de Référence	61422502/26
Date de Publication	25 février 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Ivanti Endpoint Manager Mobile (EPMM) version 12.5.0.x, 12.6.0.x et 12.7.0.x
- Ivanti Endpoint Manager Mobile (EPMM) version 12.5.1.0 et 12.6.1.0

Identificateurs externes

- CVE-2026-1281 CVE-2026-1340

Bilan de la vulnérabilité

Deux vulnérabilités critiques affectant Ivanti Endpoint Manager Mobile (EPMM) qui ont fait l'objet du bulletin de sécurité de la DGSSI « 60503001/26 » sont activement exploitées. Un attaquant peut prendre avantage de ces vulnérabilités pour exécuter du code arbitraire à distance sans authentification.

Solution

Veuillez se référer au bulletin de sécurité d'Ivanti pour l'obtention des correctifs.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risque

- Exécution de code arbitraire à distance

Indices de compromission

- 23[.]227[.]199[.]80 (Port 443)
- 64[.]7[.]199[.]177 (Ports 10882, 18899)
- 83[.]138[.]53[.]139
- 84[.]72[.]235[.]18 (Port 443)
- 86[.]106[.]143[.]200 (Port 443)
- 91[.]193[.]19[.]12 (Port 443)
- 107[.]173[.]231[.]201 (Port 6666)
- 130[.]94[.]41[.]206 (Ports 8082, 10808)
- 138[.]226[.]247[.]241
- 144[.]172[.]106[.]4
- 146[.]70[.]41[.]193 (Port 443)
- 152[.]32[.]173[.]138
- 158[.]247[.]199[.]185 (Port 80)
- 185[.]173[.]235[.]232
- 192[.]242[.]184[.]234
- 193[.]242[.]184[.]234 (Port 443)
- 194[.]78[.]67[.]253 (Port 443)
- 198[.]13[.]158[.]58 (Port 8443)
- 204[.]251[.]198[.]205 (Port 443)
- [subdomain].gobygo[.]net
- [subdomain].introo[.]sh
- [subdomain].ngrok-free[.]app
- [subdomain].main[.]interacth3[.]io
- [subdomain].ddns[.]1433[.]eu[.]org
- [subdomain].oast[.]live
- [subdomain].oast[.]me
- [subdomain].oast[.]site

- [subdomain].eyes[.]sh
- [subdomain].requestrepo[.]com
- [subdomain].ceye[.]io
- interact[.].gateway[.]horizon3ai[.]com
- hxxp://152[.]32[.]173[.]138/U26d86f1899513347.5b5b0c1b
- hxxp://64[.]7[.]199[.]177:18899
- zeetcckhtudizieudqyck5o4ez16y973h[.]oast[.]fun/
- hxxp://152[.]32[.]173[.]138/U5213b63dda61af48.0F3Ab3D3
- hxps://e598292a5fbd[.]ngrok-free[.]app/
- /mi/tomcat/webapps/mifs/401.jsp
- /mi/tomcat/webapps/mifs/403.jsp
- /mi/tomcat/webapps/mifs/1.jsp
- agent[.]sh
- /mi/tomcat/webapps/mifs/css/test.css
- /mi/tomcat/webapps/mifs/css/poc.css
- /mi/tomcat/webapps/mifs/css/cssaaa.css
- /mi/tomcat/webapps/mifs/css/login.css

Référence

Bulletin de sécurité d'Ivanti:

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

Rapport d'UNIT42 de Palo alto :

- https://unit42.paloaltonetworks.com/ivanti-cve-2026-1281-cve-2026-1340/