Security Advisory Ivanti Endpoint Manager Mobile (EPMM) (CVE-2026-1281 & CVE-2026-1340)

Primary Product
Ivanti Endpoint Manager Mobile (Core)

Categories
Security

Created Date
Jan 29, 2026 6:38:15 PM

Last Modified Date
Mar 31, 2026 11:57:05 PM

Update 29 Jan: Step by Step RPM Install KB (https://forums.ivanti.com/s/article/EPMM---How-to-Install-rpm-patch-file-for-CVE) included
Update 4 Feb: Fixed in Security Update: 0S-4 and 0L-4 included
Update: 6 Feb: RPM detection script available to help customers assess potential impact. Technical Analysis updated with reliable Indicators of Compromise (IoC's). Both in partnership with NCSC-NL.
Update 10 Feb: Guidance provided on False Positives
Update 12 Feb: RPM detection script has been updated with additional IoC's.
Update 18 Feb: Additional RPM package available which addresses a performance issue encountered by some customers.
Update 27 Feb: FAQ section updated.
Update 2 Mar: Step by Step RPM v1.1 Install KB (https://hub.ivanti.com/s/article/EPMM---How-to-Install-RPM-Patch-File-v1-1-for-CVE-2026-1281-CVE-2026-1340) included

Summary

Ivanti has released updates for Endpoint Manager Mobile (EPMM) which addresses two critical severity vulnerabilities. Successful exploitation could lead to unauthenticated remote code execution.

We are aware of a very limited number of customers whose solution has been exploited at the time of disclosure.

This vulnerability does not impact any other Ivanti products, including any cloud products, such as Ivanti Neurons for MDM. Ivanti Endpoint Manager (EPM) is a different product and also not impacted by these vulnerabilities. Customers using an Ivanti cloud product with Sentry are also not impacted by this vulnerability.

Vulnerability Details:

CVE Number	Description	CVSS Score (Severity)	CVSS Vector	CWE
CVE-2026-1281	A code injection in Ivanti Endpoint Manager Mobile allowing attackers to achieve unauthenticated remote code execution.	9.8 (Critical)	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CWE-94
CVE-2026-1340	A code injection in Ivanti Endpoint Manager Mobile allowing attackers to achieve unauthenticated remote code execution.	9.8 (Critical)	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CWE-94

Affected Versions

Product Name	Affected Version(s)	Affected CPE(s)	Resolved Version(s)	Patch Availability

Ivanti Endpoint Manager Mobile	12.5.0.0 and prior 12.6.0.0 and prior 12.7.0.0 and prior	cpe:2.3:a:ivanti:endpoint_manager_mobile:12.7.0.0:*:*:*:*:*:*:*	RPM 12.x.0.x	https://support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0S-5.noarch.rpm (https://support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0S-5.noarch.rpm)
Ivanti Endpoint Manager Mobile	12.5.1.0 and prior 12.6.1.0 and prior	cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.1.0:*:*:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.1.0:*:*:*:*:*:*:*	RPM 12.x.1.x	https://support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0L-5.noarch.rpm (https://support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0L-5.noarch.rpm)

Solution

Update 18 Feb:
An additional RPM package is available in the download portal for customers.

- (Ivanti Security Update 1761642-1.1.0S-5 (https://support.mobileiron.com/mi/vsp/AB1786671/ivanti-security-update-1761642-1.1.0S-5.noarch.rpm))
    - Applicable Versions: 12.5.0.x, 12.6.0.x and 12.7.0.x
    - Compatible Versions: 12.3.0.x and 12.4.0.x
- (Ivanti Security Update 1761642-1.1.0L-5 (https://support.mobileiron.com/mi/vsp/AB1786671/ivanti-security-update-1761642-1.1.0L-5.noarch.rpm))
    - Applicable Versions: 12.5.1.0 and 12.6.1.0

This RPM package fixes a performance issue that has been encountered by a limited number of customers. If you are not having this performance issue, you can remain on the RPM package you currently have installed. All RPMs released fully fix the security vulnerabilities.

Below you can find syntax to run the patch:

- install rpm url https://username:password@support.mobileiron.com/mi/vsp/AB1786671/ivanti-security-update-1761642-1.1.0S-5.noarch.rpm (https://username:password@support.mobileiron.com/mi/vsp/AB1786671/ivanti-security-update-1761642-1.1.0S-5.noarch.rpm)

OR

- install rpm url https://username:password@support.mobileiron.com/mi/vsp/AB1786671/ivanti-security-update-1761642-1.1.0L-5.noarch.rpm (https://username:password@support.mobileiron.com/mi/vsp/AB1786671/ivanti-security-update-1761642-1.1.0L-5.noarch.rpm)

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.

No downtime is required to apply this patch, and we are not aware of any feature functionality impact with this patch.

RPM_12.x.0.x Applicable versions: 12.5.0.x, 12.6.0.x and 12.7.0.x

- Compatible Versions: 12.3.0.x and 12.4.0.x

Note*: This issue is also fixed in - **EPMM_RPM_12.x.0 - Security Update -1761642-1.0.0S-4**

RPM_12.x.1.x Applicable Versions: 12.5.1.0 and 12.6.1.0

Note*: This issue is also fixed in - **EPMM_RPM_12.x.1 - Security Update -1761642-1.0.0L-4**

Important: the RPM script does not survive a version upgrade. If after applying the RPM script to your appliance, you upgrade to a new version you will need to reinstall the RPM. The permanent fix for this vulnerability will be included in the next product release: 12.8.0.0.

Customers need to prefix the support.mobileiron.com credentials while using the install rpm command.

Below you can find the Syntax to run the patch:

- install rpm url https://username:password@support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0S-5.noarch.rpm (https://support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0S-5.noarch.rpm)

OR

- install rpm url https://username:password@support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0L-5.noarch.rpm (https://username:password@support.mobileiron.com/mi/vsp/AB1771634/ivanti-security-update-1761642-1.0.0L-5.noarch.rpm)

The username and password are the customers software download credentials. For more detailed instructions, please leverage the following steps (https://forums.ivanti.com/s/article/EPMM---How-to-Install-rpm-patch-file-for-CVE) for RPM 1.0 or these steps (https://hub.ivanti.com/s/article/EPMM---How-to-Install-RPM-Patch-File-v1-1-for-CVE-2026-1281-CVE-2026-1340)for RPM 1.1. Either RPM provides full protection.
We strongly encourage all EPMM customers to adopt version 12.8.0.0 once it has been released later in Q1 2026. Once you have upgraded to 12.8.0.0, you will not need to reapply the RPM script.

We are providing Technical Analysis that includes affected endpoint specifics and log analysis guidance which can be found HERE (https://forums.ivanti.com/s/article/Analysis-Guidance-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340) to support investigation and forensics.

Customers should determine their own risk appetite when securing their environment. The most conservative approach, regardless of exploitation, would be to build a replacement EPMM and then migrate data to the device. You can find instructions on how to do this HERE (https://forums.ivanti.com/s/article/EPMM-Rebuild-the-EPMM-with-options). This does not require re-enrollment of devices.

Exploitation Detection RPM Package

An Exploitation Detection RPM package is now available for customers as a tool to help them assess potential exploitation. Customers can run the RPM package on their appliance. After running the tool, the customer can download the SHOWTECH logs (https://forums.ivanti.com/s/article/How-To-Collect-a-Core-Show-Tech-7121) to obtain the output of the tool. Customers should then review the output with their security team to verify the results and determine potential impact. The RPM tool looks for specific indicators related to known malicious activity.

Any suspicious behavior observed prior to the patch installation should be considered indicative of a potential compromise and should be reviewed with your forensic provider. Suspicious activity detected by the RPM script or seen in your logging after the patch has been installed may be attributed to scanning attempts and can be disregarded as a false positive.

While high-fidelity, the absence of indicators does not confirm the system has not been impacted. Please use the tool in conjunction with the analysis guidance and your own review of your security tools.

Please note: the following is an example of what the log file will look like once it is created. It will be located in the root of the /log directory in the showtech and be formatted as:

ivanti_checks_v1.0.8_<FQDN of EPMM-Date/Time stamp>.log (eg. ivanti_checks_v1.0.8_epmm.domain.com_2026-02-06_17-20-55.log)

We are providing direct links to the package (SSO is not required). Please review below to ensure you run the appropriate script in your version:

Instructions can be found HERE (https://download.ivanti.com/downloads/EPMM/Steps%20to%20Install%20RPM.txt).

Ivanti-Host-EPMM-Scan-v2-0S-2 (https://download.ivanti.com/downloads/EPMM/Ivanti-Host-EPMM-Scan-v2-0S-2/ivanti-host-scan-1.0.10S-2.noarch.rpm) (Updated 12 February)

- Applicable Versions: 12.5.0.x, 12.6.0.x and 12.7.0.x

*Compatible Version: 12.3.0.x, 12.4.0.x

Ivanti-Host-EPMM-Scan-v2-0L-2 (https://download.ivanti.com/downloads/EPMM/Ivanti-Host-EPMM-Scan-v2-0L-2/ivanti-host-scan-1.0.10L-2.noarch.rpm) (Updated 12 February)

Applicable Versions: 12.5.1.0 and 12.6.1.0

We would like to sincerely thank NCSC-NL for the pleasant and professional collaboration. They have made a significant contribution to the development of the script.

Note: Ivanti is dedicated to ensuring the security and integrity of our enterprise software products. We recognize the vital role that security researchers, ethical hackers, and the broader security community play in identifying and reporting vulnerabilities. Visit HERE (https://www.ivanti.com/support/contact-security) to learn more about our Vulnerability Disclosure Policy.

FAQ

1. Are you aware of any active exploitation of these vulnerabilities?
We are aware of a very limited number of customers who have been exploited at the time of disclosure. However, a POC was made available by a third party shortly after disclosure. We urge all customers to apply the patch as soon as possible and run the Exploitation Detection RPM package as a tool to assist in identifying potential compromise.

2. How can I tell if I have been compromised?

On 6 February we have added reliable Indicators of Compromise to our Technical Analysis. These are being shared in collaboration with NCSC-NL. We are providing a Technical Analysis for defenders HERE (https://forums.ivanti.com/s/article/Analysis-Guidance-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340).

3. If I run the Exploitation Detection RPM, can I safely assume that my appliance is clean?

No, this is an effective tool at assisting customers identifying potential compromise, however, it should be used in conjunction with other tools. Customers should review the output with their security team to verify the results and determine potential impact. The RPM tool looks for specific indicators related to known malicious activity. While high-fidelity, the absence of indicators does not confirm the system has not been impacted. Please use the tool in conjunction with the analysis guidance and your own review of your security tools.

4. Is Sentry vulnerable?

No, Sentry does not contain this vulnerability, however you should always review the security of the Sentry appliance at the same time as EPMM due to the dependency it has on the EPMM appliance and configuration.

Customers who use Sentry with a cloud product are not impacted by this vulnerability.

5. Is Ivanti Neurons for MDM vulnerable?

No. Ivanti Neurons does not contain this vulnerability. Ivanti cloud solutions are not impacted by this vulnerability.

6. What actions have Ivanti taken in response to this discovery?

In addition to rapidly and proactively providing a patch, Ivanti has mobilized additional resources and support teams to assist customers and is actively collaborating with security partners, the broader security community and law enforcement.

7. Will HA sync apply the RPM patch to our secondary core if a secondary core is being used?

No, the RPM patch needs to be applied to each core separately. HA Sync will not apply the patch to any secondary cores automatically.

8.. Do I need to apply both RPM patches?

No. The RPM patches are version specific, not vulnerability specific. You only need to apply the RPM patch that corresponds with your version.

9. How do I validate if the RPM was applied successfully?

When the RPM is installed, there will be a response line indicating success. An error of any kind will be generated if there's an issue with the application.

10. Can private certificates from mobile devices we manage be exfiltrated?

No. Private certificates from a mobile device under management by EPMM cannot leave the device. They cannot be exfiltrated or stolen.

We recommend in our Technical Analysis (https://hub.ivanti.com/s/article/Analysis-Guidance-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US) to rotate EPMM appliance certificates, but this does not apply to private certificates on mobile devices under management by EPMM because they cannot be stolen.

11. Can an attacker run mobile commands on the mobile devices managed by EPMM?

No. You cannot run mobile commands on devices managed by EPMM, this is not how EPMM works. As covered in our Technical Analysis (https://hub.ivanti.com/s/article/Analysis-Guidance-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US), we do recommend reviewing any new policies pushed to users when threat hunting, but this would not allow a threat actor to run a mobile command on the devices.

12. What should I do if I need help?

If you have questions after reviewing this information, you can log a case and/or request a call via the Success Portal (https://success.ivanti.com/Community_RegStep1_Page?inst=UL) .

Article Number : 000104594

Article Promotion Level

Normal