

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Ivanti Addressed A Critical Zero-Day Flaw in EPMM Software**

Date of Publication

July 26, 2023

Admiralty Code

A1

TA Number

TA2023314




# Summary

**First Seen:** July 24, 2023

**Affected Platforms:** Ivanti Endpoint Manager Mobile

**Impact:** The vulnerability allows unauthorized remote access to personal information and enables limited server changes, posing significant security risks to affected organizations.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-35078	Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	Ivanti Endpoint Manager Mobile			

# Vulnerability Details

## #1

Ivanti, a U.S. IT software company, has addressed a critical zero-day authentication bypass vulnerability, identified as CVE-2023-35078, in their mobile device management software known as Endpoint Manager Mobile (EPMM). The vulnerability allowed unauthorized remote actors to potentially access users' personal information and make limited changes to the server, posing a significant security risk.

## #2

All supported versions of Ivanti EPMM, including 11.4 releases 11.10, 11.9, and 11.8, are affected, as well as older versions and releases. Ivanti confirmed that the vulnerability was not introduced maliciously and was not part of a supply chain attack.

## #3

A small number of customers, less than 10, were reported to have fallen victim to attacks exploiting the vulnerability. Over 2,900 Ivanti EPMM user portals were found exposed online, with some linked to U.S. local and state government agencies.

## #4

The Norwegian government ministries were the first known victims of the attack. The breach raised concerns about potential access to sensitive data on compromised systems.

## #5

Ivanti has released security patches to address the vulnerability, and users are advised to promptly upgrade to fixed versions (11.8.1.1, 11.9.1.1, and 11.10.0.2) or higher. To detect exploitation, users can check logs for any targeted activity on the API v2 endpoint, which was accessible without authentication in vulnerable versions.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-35078	Ivanti Endpoint Manager Mobile	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*	CWE-287

# Recommendations



**Apply Security Patches:** Immediately update the Ivanti EPMM software to the fixed versions 11.8.1.1, 11.9.1.1, or 11.10.0.2. These patches address the zero-day vulnerability and protect the system from exploitation.



**Monitor Logs for Suspicious Activity:** Regularly review logs to detect any unauthorized access to the API v2 endpoint. Be vigilant for unusual API calls, especially those attempting to access the endpoint without authentication, as this indicates potential exploitation attempts.



**Restrict API Access:** Implement access controls and restrictions for the API v2 endpoint to ensure that only authorized users can access it. By limiting access, you reduce the attack surface and make it more difficult for malicious actors to exploit the vulnerability.

# Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation
<b><u>TA0010</u></b> Exfiltration	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1588.005</u></b> Exploits
<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1190</u></b> Exploit Public-Facing Application		

## Patch Details

The vulnerability (CVE-2023-35078) has been fixed in the following versions of Ivanti EPMM:

- Ivanti EPMM version 11.8.1.1
- Ivanti EPMM version 11.9.1.1
- Ivanti EPMM version 11.10.0.2

## References

[https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en\\_US](https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US)

<https://www.ivanti.com/blog/cve-2023-35078-new-ivanti-epmm-vulnerability>

<https://www.cisa.gov/news-events/alerts/2023/07/24/ivanti-releases-security-updates-endpoint-manager-mobile-epmm-cve-2023-35078>

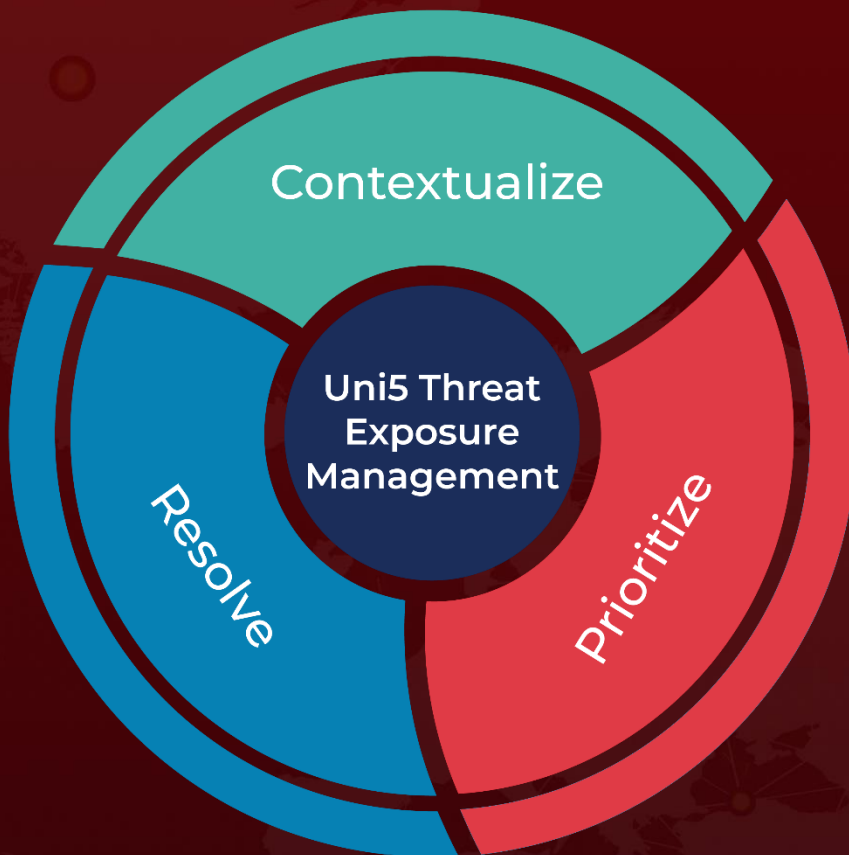
<https://twitter.com/wdormann/status/1683488594084724738>

<https://nsm.no/aktuelt/nulldagssarbarhet-i-ivanti-endpoint-manager-mobileiron-core>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**July 26, 2023 • 5:30 AM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)