



Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability

Zero-day vulnerabilities exploited in the wild

<https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability>

CVEs: CVE-2023-35081, CVE-2023-35078

Ivanti Endpoint Manager Mobile (EPMM, formerly MobileIron Core) contains an authentication bypass vulnerability (CVE-2023-35078) that allows unauthenticated access to specific API paths and a path traversal vulnerability (CVE-2023-35081). An attacker with access to these API paths can access personally identifiable information (PII) such as names, phone numbers, and other mobile device details for users on a vulnerable system. An attacker can also make other configuration changes including installing software and modifying security profiles on registered devices.

Background

Ivanti Endpoint Manager Mobile (EPMM) is a software used to manage endpoints running specifically mobile devices running on iOS, Android etc. Successful exploitation could lead to various security risks, including but not limited to:

- Unauthorized access to sensitive information stored within Ivanti EPMM
- Unauthorized administrative actions, compromising the integrity and availability of the data and resources
- Unintended disclosure of confidential data

Announced

July 24, 2023: The Norwegian National Security Authority (NSM) has confirmed that attackers used a zero-day vulnerability in Ivanti's Endpoint Manager Mobile (EPMM) solution to breach a software platform used by 12 ministries in the country.

July 31, 2023: CISA issued an advisory regarding the vulnerability, and add the vulnerabilities into their Known Exploited Vulnerabilities (KEV) list.

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-213a>

Latest Developments

In response to the identified vulnerabilities, Ivanti has released patches for versions 11.8.1.1, 11.9.1.1, and 11.10.0.

CVE-2023-35081:

<https://forums.ivanti.com/s/article/KB-Arbitrary-File-Write-CVE-2023-35081>

CVE-2023-35078:

<https://forums.ivanti.com/s/article/KB-Remote-unauthenticated-API-access-vulnerability-CVE-2023-35078>

Aug 8, 2023: FortiGuard Labs released IPS signature to address the vulnerability (CVE-2023-35078) and detect any attack attempts. IPS signature for the vulnerability (CVE-2023-35081) is currently being investigated. It is strongly recommended to apply patches as per vendor notes.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

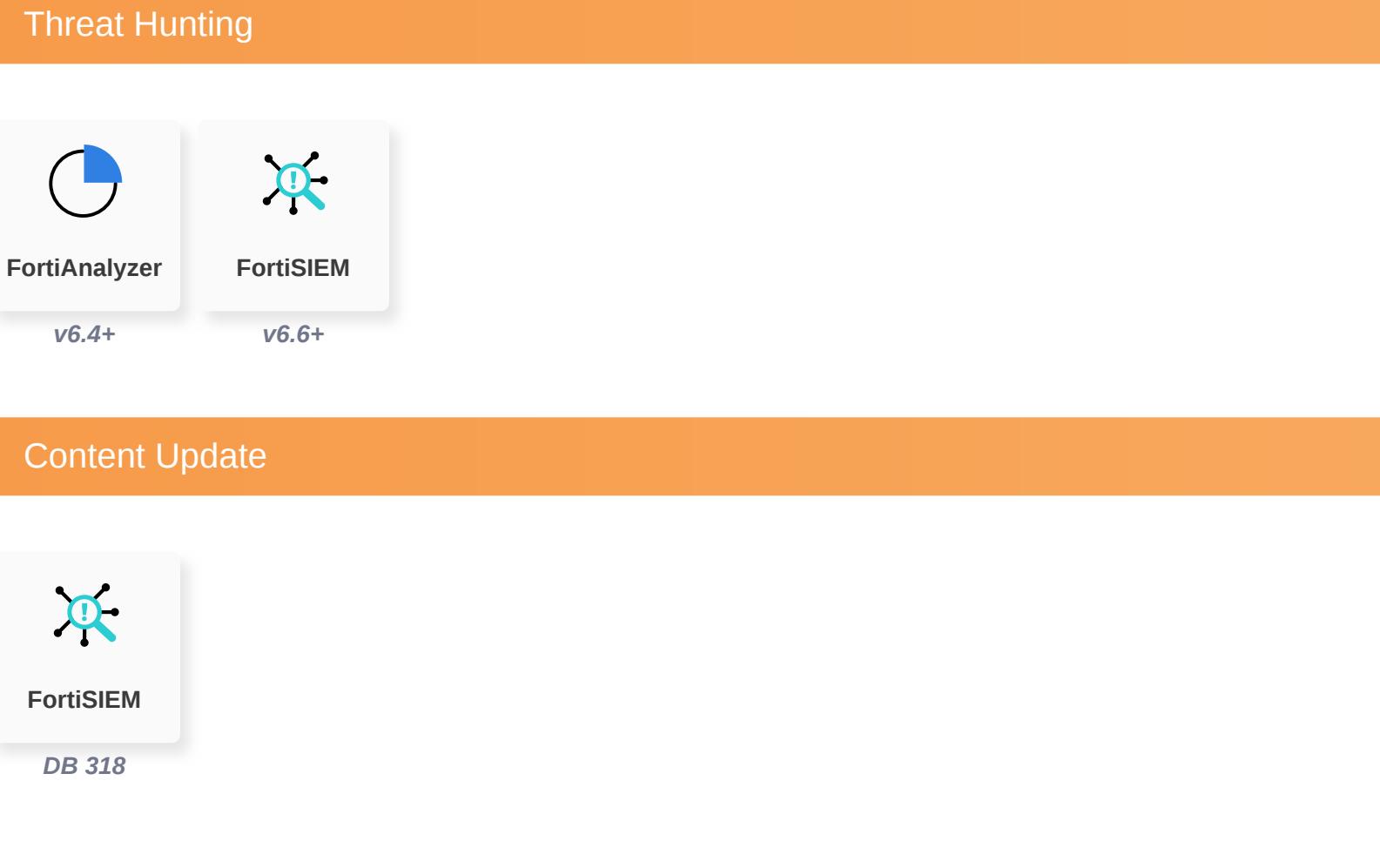
Reconnaissance

Weaponization

Delivery

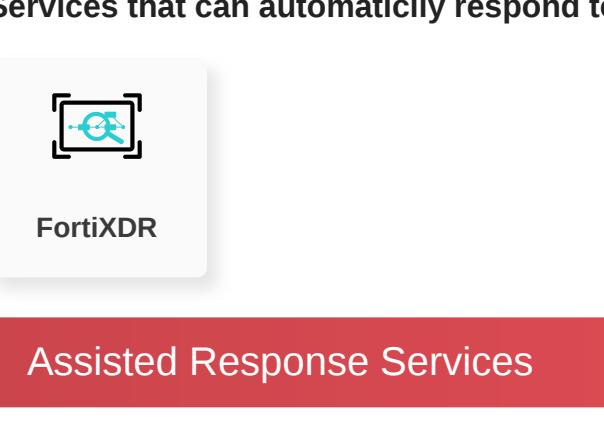
AV

Detects known malware related to Ivanti Endpoint Manager Mobile (CVE-2023-35078 and CVE-2023-35081)



AV (Pre-filter)

Detects known malware related to Ivanti Endpoint Manager Mobile (CVE-2023-35078 and CVE-2023-35081)



Exploitation

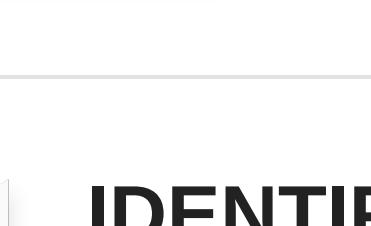
IPS

Detects and blocks attack attempts targeting Ivanti Endpoint Manager Mobile (CVE-2023-35078)



Web App Security

Detects and blocks attack attempts targeting Ivanti Endpoint Manager Mobile (CVE-2023-35078)



Installation

C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection



Threat Hunting



Content Update

RESPOND

Develop containment techniques to mitigate impacts of security events.

Automated Response

Services that can automatically respond to this outbreak.

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Business Reputation

Know attackers next move to protect against your business branding.

Additional Resources

Bleeping Computer

<https://www.bleepingcomputer.com/news/security/ivanti-discloses-new-critical-auth-bypass-hug-in-mobileiron-core/>

The Hacker News

<https://thehackernews.com/2023/07/ivanti-releases-urgent-patch-for-epmm.html>

The Record

<https://therecord.media/ivanti-urges-customers-to-apply-patch/>

Learn more about [FortiGuard Outbreak Alerts](#)

