CVE-2023-35078 – HILFE ZUR SELBSTHILFE

Erste Schritte zur Behandlung der Sicherheitslücke CVE-2023-35078 in Ivanti Endpoint Manager Mobile (EPMM)

Stand: Version 4.0, 10.08.2023, 15:00

SACHVERHALT

Am 24.07.2023 hat das Unternehmen Ivanti Informationen zu einer Sicherheitslücke in ihrer Endpoint Manager Mobile (EPMM) Software veröffentlicht (auch bekannt als MobileIron Core). Diese Schwachstelle ermöglicht unbefugten Dritten, ohne Anmeldung, auf die API-Schnittstelle der Software zuzugreifen.[1] Die Ausnutzung erfolgt über das HTTPS-Protokoll.[2]

Laut der Meldung[3] der Cybersecurity & Infrastructure Security Agency (kurz CISA) können die Angreifer über diesen Weg Zugriff auf beispielsweise Namen, Telefonnummern und weitere Geräteeigenschaften erhalten. Darüber hinaus hat der Angreifer die Möglichkeit einen administrativen Account in EPMM zu erstellen und somit privilegierte Rechte zu erlangen, um zum Beispiel die Konfiguration zu verändern, weitere Nutzer anzulegen oder anderweitige kritische, möglicherweise betriebsstörende Änderungen vorzunehmen.

Die aktuelle Schwachstelle wird nach dem Common Vulnerability Scoring System (CVSS) zur Einschätzung von IT-Sicherheitslücken mit 10.0 bewertet (dem höchst möglichen Score) und ist somit als kritisch klassifiziert.

Am 29.07.2023 wurde auf GitHub ein Proof on Concept (PoC) Code veröffentlicht, der ermöglicht zu prüfen, ob eine Ivanti Instanz verwundbar ist. Weiterhin wurde ein Proof of Concept Exploit zum Ausnutzen der Schwachstelle veröffentlicht. Sofern der Patch nach dem 29.07.2023 eingespielt wurde, empfehlen wir eine Untersuchung des Systems, da mithilfe dieser PoCs das Ausnutzen der Schwachstelle ohne tieferes technisches Wissen möglich ist.

Zusätzlich wurde am 28.07.2023 von Ivanti eine weitere Sicherheitslücke (CVE-2023-35081) publiziert. Hierbei handelt es sich um eine Schwachstelle, welche es dem Angreifer erlaubt, als authentifizierter Administrator beliebige Schreibvorgänge auf dem EPMM-Server durchzuführen.

Durch die Kombination der beiden Schwachstellen ist es möglich, die Administratorauthentifizierung und ACL-Einschränkungen zu umgehen und Dateien auf dem System zu hinterlegen. Angreifer könnten diese Schwachstelle letztendlich zur Ausführung von Betriebssystembefehlen im Kontext des Tomcat-Benutzers nutzen.[4]

[1] https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US
[2] https://socradar.io/critical-zero-day-in-ivanti-epmm-formerly-mobileiron-core-is-actively-exploited-cve-2023-35078/
[3] https://www.cisa.gov/news-events/alerts/2023/07/24/ivanti-releases-security-updates-endpoint-manager-mobile-epmm-cve-2023-35078
[4] https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US

HISOLUTIONS

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

Fon: +49 30 533 289-0
Fax: +49 30 533 289-900

Am 03.08.2023 wurde eine weitere Sicherheitslücke (CVE-2023-35082) in Endpoint Manager Mobile (EPMM) veröffentlicht. Die Schwachstelle weist ebenfalls eine CVSS-Bewertung von 10.0 auf und ist somit ebenfalls als **kritisch** klassifiziert. Am 07.08.2023 hat Invanti veröffentlicht, dass diese Schwachstelle alle Versionen von EPMM betrifft.[5] Die Schwachstelle ist ähnlich zu CVE-2023-35078 und erlaubt unbefugten Dritten, ohne Anmeldung, auf die API-Schnittstelle der Software zuzugreifen.

HINWEIS: Im Folgenden werden die aktuell verfügbaren Informationen genutzt, um eine mögliche Vorgehensweise zur Behebung und Überprüfung der Ausnutzung der Schwachstelle zu definieren. Das Dokument wird laufend aktualisiert. Bitte achten Sie daher auch auf weitere Veröffentlichungen unter https://research.hisolutions.com/. Weitere Informationen erhalten Sie auch beim Bundesamt für Sicherheit in der Informationstechnik (BSI) unter:

- https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2023/2023-249317-1032.pdf?__blob=publicationFile&v=2
- https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2023/2023-257569-1032.pdf?__blob=publicationFile&v=3.

BETROFFENE SYSTEME

Laut den Hinweisen des Herstellers sind die folgenden Versionen bzw. Releases von der CVE-2023-35078 betroffen:

Betroffene Versionen (CVE-2023-35078)	Bereitgestellte Updates
11.10.0.1 und niedriger	11.10.0.2 oder aktueller
11.9.1.0 und niedriger	11.9.1.1 oder aktueller
11.8.1.0	11.8.1.1 oder aktueller
11.7 und niedriger	Update auf neuere Version, bevorzugt auf 11.10

Laut den Hinweisen des Herstellers sind die folgenden Versionen bzw. Releases von der CVE-2023-35082 betroffen:

Betroffene Versionen (CVE-2023-35082)	Bereitgestellte Updates
11.10	11.10.0.3 **und** RPM Skript
11.9	11.9.1.2 **und** RPM Skript
11.8	11.8.1.2 **und** RPM Skript
11.7 und niedriger	Update auf neuere Version, bevorzugt auf 11.10, inklusive Update für die CVE-2023-35078 **und** RPM Skript

Die Sicherheitslücke CVE-2023-35082 wird final mit dem kommenden Release 11.11 geschlossen.

[5] https://forums.ivanti.com/s/article/CVE-2023-35082-Remote-Unauthenticated-API-Access-Vulnerability-in-MobileIron-Core-11-2-and-older?language=en_US

SCHRITTE ZUR BEHANDLUNG DER SCHWACHSTELLE

HINWEIS: Die folgenden Schritte beinhalten Maßnahmen, welche von technisch geschultem Personal durchgeführt werden sollten. Bitte geben Sie dieses Dokument im Zweifel an Ihren IT-Dienstleister, welcher zusammen mit Ihnen diese Schritte abarbeiten kann.

Schritt 1: Verhindern weiterer Angriffe

Da die Schwachstelle aktiv ausgenutzt wird, empfehlen wir vor der Überprüfung einer möglichen Kompromittierung den folgenden Schritt durchzuführen, um eine akute Infektion oder Ausbreitung zu verhindern:

- Unterbrechen Sie die netzwerkseitige Erreichbarkeit des Ivanti-Servers (insbesondere aus dem Internet) bis die Analyse des Servers abgeschlossen ist und der aktuelle Patch installiert ist.

Schritt 2: Überprüfen einer möglichen Kompromittierung

Um eine mögliche Kompromittierung Ihrer Systeme überprüfen zu können, befolgen Sie die folgenden Schritte:

1. Erstellen Sie eine Sicherung (Backup oder Snapshot) des Ivanti-Servers und exportieren Sie die Audit- und Webserver-Logs (`http-access_log`, `http-request_log`, `https-access_log`, `https-request_log`).
2. Sollten Sie Direktkunde bei Ivanti sein, fragen Sie bei Ivanti die vertrauliche Untersuchungsanleitung an. Sollten Sie die Software über einen Reseller bezogen haben, kontaktieren Sie diesen mit der Bitte, die Unterlagen für Sie bei Ivanti anzufragen.
3. Prüfen Sie die Konfiguration des Ivanti EPMM auf unbekannte Änderungen. Überprüfen Sie insbesondere, ob neue oder unbekannte (administrative) Konten angelegt wurden.[6]
4. Prüfen Sie die Ivanti EPMM Audit-Logs auf unbekannte Aktivitäten und Anomalien.
5. Prüfen Sie die Webserver-Logs auf die folgenden Teilstrings:
   5.1. `/mifs/aad/api/v2/`[7] für die CVE-2023-35078
   5.2. `/mifs/asfV3/api/v2/`[8] für die CVE-2023-35082

   Hinweis: Erfolgreiche Anfragen weisen einen HTTP Status Code von 200 auf. Überprüfen Sie die aufgerufenen API-Endpunkte. Der Endpunkt „`ping`“ wird häufig genutzt, um zu überprüfen, ob der Server von der CVE-2023-35082 oder der CVE-2023-35078 betroffen ist – es handelt sich damit um keinen Indikator für eine Kompromittierung.
6. Untersuchen Sie Ihr System auf neu angelegte Dateien.[9]
7. Prüfen Sie die vom Tomcat-Benutzer ausgeführten Prozesse auf Anomalien.
8. Prüfen Sie alle Logs auf Anomalien im Zusammenhang mit dem Tomcat-Benutzer.

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

[7] https://www.rapid7.com/blog/post/2023/07/26/etr-cve-2023-35078-critical-api-access-vulnerability-ivanti-in-endpoint-manager-mobile/

[8] https://www.rapid7.com/blog/post/2023/08/02/cve-2023-35082-mobileiron-core-unauthenticated-api-access-vulnerability/

[9] https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US

Schritt 3: Maßnahmenempfehlungen

Keine Kompromittierung

Sofern in der Analyse keine Auffälligkeiten festgestellt werden konnten, führen Sie die folgenden Schritte aus:

- Spielen Sie für die Behebung der CVE-2023-35078 Updates des Ivanti EPMM auf eine der aktuellen Versionen 11.8.1.1, 11.9.1.1 oder 11.10.0.2 ein. Für ältere Versionen/Releases steht ein RPM bereit.[10] Ein Update von älteren Versionen auf eine neuere Version (bevorzugt 11.10) ist empfohlen, um auch die weitere Sicherheitslücke CVE-2023-35082 schließen zu können.
- Für die Behebung von CVE-2023-35082 stellt Ivanti ein RPM Skript für aktuelle Versionen von EPMM bereit. Das Skript behebt lediglich die CVE-2023-35082, daher ist es empfohlen vorher den Patch für die CVE-2023-35078 einzuspielen. Weiterhin ist das RPM Skript nur für Version 11.3 oder neuer anwendbar. Ältere Releases müssen entsprechend vorher aktualisiert werden. Final wird die Schwachstelle mit dem kommenden Release 11.11 geschlossen.[11]

Kompromittierung

Sofern in der Analyse Spuren einer Kompromittierung festgestellt wurden, empfehlen wir die folgenden Schritte:

- Führen Sie eine weiterführende forensische Untersuchung zur Beantwortung der folgenden Analysefragen durch:
  - Welche Aktionen wurden über die API durchgeführt?
  - Hat sich der Angreifer weitere Zugänge verschafft?
  - Hat sich der Angreifer im Netzwerk weiterbewegt?
  - Kann der Angreifer an Domänen User Credentials gelangt sein?
- Setzen Sie je nach Ergebnis der forensischen Analyse einen Maßnahmenplan um, der einen sicheren Betrieb ermöglicht. Dazu gehört ein potenzielles Neuaufsetzen des Servers oder ein Wiedereinspielen eines Backups, das vor dem Datum der initialen Kompromittierung erstellt wurde.
- Ändern Sie Passwörter und setzen Sie Zertifikate zurück, die durch den Angriff ausgelesen worden sein könnten.
- Prüfen Sie gemeinsam mit Ihrem/r Datenschutzbeauftragten, welchen Informationspflichten nachzukommen ist.

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

[11] https://forums.ivanti.com/s/article/KB-Remote-Unauthenticated-API-Access-Vulnerability-CVE-2023-35082?language=en_US