



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Weitere kritische Schwachstelle in Ivanti Endpoint Manager Mobile (EPMM) und MobileIron Core

CSW-Nr. 2023-257569-1132, Version 1.1, 09.08.2023

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Nachdem das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits im Juli vor einer Verwundbarkeit des Endpoint Manager Mobile (EPMM) – ehemals vertrieben unter dem Namen MobileIron Core – gewarnt hatte [BSI2023], veröffentlichte der Hersteller Ivanti am 3. August 2023 Informationen zu einer weiteren Sicherheitslücke in diesem Produkt. Die Sicherheitslücke wird gemäß Common Vulnerabilities and Exposures (CVE) unter der Nummer CVE-2023-35082 gelistet und hat erneut eine CVSS-Bewertung von 10.0 ("kritisch").

Zunächst wurden nur die End-of-Life (EoL) Versionen von EPMM bzw. MobileIron Core kleiner 11.3 als betroffen aufgeführt. Am 7. August veröffentlichte Ivanti jedoch ein Update zu dem Security Advisory [IVAN2023a], wonach nun **alle Versionen** von Ivanti EPMM bzw. MobileIron Core durch CVE-2023-35082 verwundbar sind.

Die Schwachstelle ist ähnlich zu der kürzlich bekanntgewordenen und aktiv ausgenutzten Schwachstelle CVE-2023-35078 [BSI2023]. Sie ermöglicht einem nicht-authentifizierten Angreifer aus dem Internet den Zugriff auf die API Endpunkte (Authentication Bypass). Der Zugriff auf die API kann genutzt werden, um

- * 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
 2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
 3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
 4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

an persönliche Informationen, wie Namen, Telefonnummern und andere Details zu gelangen oder um limitierte Konfigurationsänderungen vorzunehmen [IVAN2023a][IVAN2023b].

Für die betroffenen Produktversionen von EPMM bzw. MobileIron Core 11.10 bis 11.3 wird ein Skript zum Schließen der Schwachstelle von Ivanti bereitgestellt. Für die EoL-Versionen 11.2 und niedriger steht keine Mitigationsmaßnahme zur Verfügung. Es ist daher notwendig, auf eine neuere Version zu aktualisieren – vorzugsweise 11.10.

Bewertung

Die gefundene Schwachstelle CVE-2023-35082 betrifft alle Versionen von Ivanti Endpoint Manager Mobile (EPMM). Endpoint Manager Gerätemanagement Lösungen sind ein beliebtes Ziel von Angreifern, da sie in vielen Unternehmen zur Verwaltung mobiler Geräte eingesetzt werden. Die entdeckte Sicherheitslücke birgt ein hohes Risiko einer Kompromittierung verwundbarer Systeme, da sie über das Internet ohne Authentifizierung ausgenutzt werden kann.

Aufgrund der Ähnlichkeit der Schwachstelle zu CVE-2023-35078 kann von einer baldigen breiten Ausnutzung ausgegangen werden. Die Sicherheitsforscher von Rapid7 stellen in einem Blogbeitrag technische Details zur Ausnutzung und Behebung sowie ein Proof-of-Concept bereit [RAPID723]. Bislang gibt es jedoch keine Berichte über Angriffsversuche mithilfe von CVE-2023-35082.

Laut Ivanti ist die Gefahr einer Ausnutzung abhängig von der individuellen Kunden-Konfiguration. **Es ist nur möglich, die Schwachstelle über HTTP auszunutzen.** [IVAN2023b]

Update 1:

Ivanti gibt an, dass es bereits Ausnutzungen der Schwachstelle CVE-2023-35082 gab. Außerdem werden viele Server auf die Schwachstelle gescannt, meist wird hierzu der "ping" API-Endpunkt verwendet. Dies zählt technisch gesehen schon als "Ausnutzung". [IVAN2023b]

Maßnahmen

Um die Schwachstelle zu beheben und das Risiko einer Kompromittierung zu reduzieren, sollten IT-Sicherheitsverantwortliche das von Ivanti zur Verfügung gestellte RPM Skript [IVAN2023b] nutzen, um Ivanti Endpoint Manager Mobile (EPMM) bzw. MobileIron Core Server so schnell wie möglich abzusichern.

Das RPM Skript schützt nur vor CVE-2023-35082, alle früheren Lücken bleiben jedoch offen. Daher sollte zunächst auf die Versionen 11.10.0.3, 11.9.1.2 oder 11.8.1.2 aktualisiert werden. Ivanti wird mit der kommenden Release 11.11 alle bekannten Sicherheitslücken schließen. Das Skript wird nur von den EPMM Versionen 11.3 und höher unterstützt [IVAN2023b].

Zur Mitigation von CVE-2023-35082 muss wie folgt vorgegangen werden [IVAN2023b]:

- Verwenden Sie SSH, um sich über ein Terminal als Administrator anzumelden, der während der Systeminstallation erstellt wurde.
- Geben Sie das entsprechende Passwort ein.
- Geben Sie "enable" ein und verwenden Sie das Systempasswort, das während der Systeminstallation festgelegt wurde, um in den EXEC-PRIVILEGED-Modus zu gelangen. Die Befehlszeilenaufforderung ändert sich von ">" zu "#".
- Führen Sie das Aufräumskript aus, um ältere RPM-Downloads zu bereinigen. Installieren Sie dazu das RPM Skript mit dem Befehl
 - › `install rpm url https://support.mobileiron.com/ivanti-updates/ivanti-cli-cleanup-1.0.0-1.noarch.rpm`
- Installieren Sie nun das RPM-Skript zur Behebung von CVE-2023-35082 mit dem Befehl
 - › `install rpm url https://support.mobileiron.com/ivanti-updates/ivanti-security-update-3.0.0-3.noarch.rpm`
- Geben Sie `reload` ein, um das System neu zu starten.

Es ist auch möglich, zur Mitigation jeglichen HTTP-Datenverkehr zu blockieren und nur die Ports 443, 9997 und 8883 offen zu lassen, um einen Server vor einer Ausnutzung zu schützen. Weitere Informationen über mögliche Folgen bei den Mitigationsmaßnahmen finden sich im Advisory [IVAN2023b].

IT-Sicherheitsverantwortliche sollten zudem auf eine mögliche Kompromittierung prüfen. Dazu stehen folgende Indicators of Compromise (IoCs) zur Verfügung [RAPID723]:

- Die Log Datei `/var/log/httpd/http-access_log` würde bei einer Ausnutzung Einträge zeigen, in denen der betroffene API Endpunkt mit `/mifs/asfV3/api/v2/` im Pfad und ein HTTP Status Code mit 200 angegeben sind. Blockierte Angriffsversuche enthalten dagegen den HTTP Status Code 401 oder 403.
- Ähnlich ist der Fall in der Log Datei `/var/log/httpd/http-request_log`. Darin bieten Einträge mit dem Pfad `/mifs/asfV3/api/v2/` Auskunft über eine potentielle Kompromittierung.
- Einträge mit `/mifs/asfV3/api/v2/` weisen auf die Ausnutzung von CVE-2023-35082 hin, dagegen diejenigen mit `/mifs/aad/api/v2/` auf die von CVE-2023-35078.

Update 1:

Es gab einen Fehler bei der Pfadbezeichnung für CVE-2023-35078. Der API-Pfad für diese Schwachstelle lautet: `/mifs/aad/api/v2/`

Es ist zudem wichtig zu prüfen, welche API-Endpunkte genutzt wurden. Mit der API-Dokumentation lassen sich die Tätigkeiten und möglichen Datenzugriffe von Angreifenden nachvollziehen.

Zugriffe auf den "ping" API-Endpunkt werden für Scans von Angreifenden, aber auch von Sicherheitsforschenden genutzt, um zu erkennen, ob ein Server von CVE-2023-35082 oder CVE-2023-35078 betroffen ist. Pings sind kein Indikator für eine Kompromittierung - auf diese muss getrennt untersucht werden. [IVAN2023b]

Links

[BSI2023] Zero-Day Schwachstelle in IvantiEndpoint Manager Mobile geschlossen:

<https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2023/2023-249317-1032.pdf>

[IVAN2023a] Security Advisory CVE-2023-35082:

<https://forums.ivanti.com/s/article/CVE-2023-35082-Remote-Unauthorized-API-Access-Vulnerability-in-MobileIron-Core-11-2-and-older>

[IVAN2023b] Ausführlicheres Security Advisory zu CVE-2023-35082:

<https://forums.ivanti.com/s/article/KB-Remote-Unauthorized-API-Access-Vulnerability-CVE-2023-35082>

[RAPID723] CVE-2023-35082 - MobileIron Core Unauthenticated API Access Vulnerability:

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

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**

Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**

Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe

Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**

Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-ingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.