



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Zero-Day Schwachstelle in Ivanti Endpoint Manager Mobile geschlossen

CSW-Nr. 2023-249317-1132, Version 1.1, 31.07.2023

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

Am 24. Juli 2023 wurde eine Zero-Day Schwachstelle im Endpoint Manager Mobile (EPMM) – ehemals vertrieben unter dem Namen MobileIron Core – von Ivanti geschlossen. Die Sicherheitslücke wird gemäß Common Vulnerabilities and Exposures (CVE) unter der Nummer CVE-2023-35078 gelistet und hat eine CVSS-Bewertung von 10.0 ("kritisch").

Sie ermöglicht einem nicht-authentifizierten Angreifer aus dem Internet über bestimmte API-Pfade Zugriff auf persönlich identifizierbare Informationen (PII), wie Namen, Telefonnummern und andere Details, auf verwundbaren Mobilgeräten zu erlangen (Authentication Bypass). Der Angreifer kann auch Konfigurationsänderungen vornehmen, einschließlich der Erstellung eines administrativen EPMM-Benutzerkontos, das weitere Änderungen an einem verwundbaren System vornehmen kann. [IVAN2023a]

Die betroffenen Produktversionen von EPMM sind:

- 11.10,
- 11.9 und
- 11.8.

Ältere, nicht länger unterstützte Versionen, sind ebenfalls betroffen.

* 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.

Die Nationale Sicherheitsbehörde Norwegens teilte am 24. Juli 2023 mit, dass die Schwachstelle für Angriffe auf norwegische Ministerien verwendet wurde. [NSM2023]

Update 1:

Am 28. Juli 2023 wurde eine weitere Schwachstelle in Ivanti EPMM bekanntgegeben zu der ein Patch bereitsteht [IVAN2023c]. Die Schwachstelle mit der Kennung CVE-2023-35081 und einer CVSS-Bewertung von 7.2 erlaubt einen authentifizierten Administrator schadhafte Dateien auf EPMM Server zu schreiben (Arbitrary File Write) und so OS Befehle als tomcat Nutzer auszuführen. Die Schwachstelle wurde in Kombination mit CVE-2023-35078 bei Angriffen bereits ausgenutzt und betrifft ebenfalls die oben genannten Produktversionen von EPMM.

Mittlerweile wurde auch ein Proof-of-Concept auf GitHub [GITHUB23] veröffentlicht, mit dem die Verwundbarkeit eines Servers überprüft werden kann.

Bewertung

Die gefundene Schwachstelle CVE-2023-35078 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. Da bereits von Angriffen auf eine geringe Anzahl an Kunden von Ivanti EPMM berichtet wird [IVAN2023b], kann von einer weiteren Ausnutzung ungepatchter Systeme ausgegangen werden.

Maßnahmen

Um die Schwachstelle zu beheben und das Risiko einer Kompromittierung zu reduzieren, sollten IT-Sicherheitsverantwortliche die verfügbaren Updates für Ivanti Endpoint Manager Mobile (EPMM) so schnell wie möglich installieren. Außerdem sollte geprüft werden, ob weitere EPMM-Benutzerkonten durch einen möglichen Angriff angelegt wurden.

Es wird empfohlen, auf die Versionen 11.10.0.2, 11.9.1.1, 11.8.1.1 oder höher zu aktualisieren. Weitere Informationen zu Mitigationsmaßnahmen finden sich im Knowledge Base Artikel, der im Security Advisory des Herstellers [IVAN2023a] verlinkt ist. Mit den dort aufgeführten Hinweisen können auch ältere Produktversionen vor einer Kompromittierung geschützt werden.

Links

[IVAN2023a] <https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability>

[IVAN2023b] <https://www.ivanti.com/blog/cve-2023-35078-new-ivanti-epmm-vulnerability>

[IVAN2023c] <https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write>

[NSM2023] <https://nsm.no/aktuelt/nulldagssarbarhet-i-ivanti-endpoint-manager-mobileiron-core>

[GITHUB23] <https://github.com/lager1/CVE-2023-35078/>

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.