Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Zero-Day Schwachstelle in Ivanti Sentry geschlossen

CSW-Nr. 2023-257880-1032, Version 1.0, 22.08.2023

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

Am 21. August 2023 wurde eine Zero-Day Schwachstelle in Ivanti Sentry - ehemals vertrieben unter MobileIron Sentry - bekannt gegeben [IVAN2023a]. Die Sicherheitslücke wird gemäß Common Vulnerabilities and Exposures (CVE) unter der Nummer CVE-2023-38035 gelistet und hat eine CVSS-Bewertung von 9.8 ("kritisch"). Einem nicht-authentifizierten Angreifer könnte es mithilfe dieser Verwundbarkeit gelingen, auf sensible Teile der API zuzugreifen (Authentication Bypass), die zur Konfiguration von Ivanti Sentry im System Manager Portal (MICS) genutzt wird. In der Folge können die Täter Konfigurationsänderungen an Ivanti Sentry durchführen, Betriebssystem-Befehle ausführen sowie Dateien verändern oder erstellen. Ursache hierfür ist eine unzureichend restriktive Apache HTTPD-Konfiguration [IVAN2023b] [IVAN2023c].

Betroffen von CVE-2023-38035 sind die unterstützten Produktversionen 9.18, 9.17 und 9.16 sowie alle älteren, nicht länger unterstützen Versionen von Ivanti (MobileIron) Sentry.

Die Schwachstelle wurde nach erfolgreichen Angriffen auf Ivanti Endpoint Manager Mobile (CVE-2023-35078, CVE-2023-35081) bereits von Angreifern ausgenutzt [IVAN2023c], [BSI2023].

Ivanti stellt ein RPM Skript für die unterstützten Versionen zur Verfügung, um die Schwachstelle zu schließen. [IVAN2023c]

* 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.

Bewertung

Da die entdeckte Sicherheitslücke CVE-2023-38035 alle Versionen von Ivanti MobileIron Sentry betrifft und Angreifer im Rahmen der zuletzt bekanntgewordenen Verwundbarkeiten im Ivanti Endpoint Manager Mobile (EPMM) **bereits erste Angriffsziele kompromittiert haben**, birgt der Sachverhalt ein hohes Risiko – zumal die Ausnutzung über das Internet ohne Authentifizierung möglich ist.

Betroffen von der Schwachstelle sind alle Ivanti Sentry Kunden, die den Port 8443 exponieren und damit den Ivanti System Manager aus dem Internet erreichbar machen [IVAN2023c]. In Deutschland konnte eine mittlere Betroffenheit von potenziell gefährdeten Ivanti Sentry Instanzen festgestellt werden.

Technische Details oder ein Proof-of-Concept sind zum Zeitpunkt der Veröffentlichung des Advisories nicht verfügbar. Jedoch ist davon auszugehen, dass diese Schwachstelle von Angreifern, wie die Sicherheitslücken in Ivanti EPMM, schnell großflächig ausgenutzt werden könnte und es nicht bei den von Ivanti aktuell genannten einzelnen Angriffen [IVAN2023c] bleiben wird.

Maßnahmen

Um die Schwachstelle CVE-2023-38035 zu beheben und das Risiko einer Kompromittierung zu reduzieren, sollten IT-Sicherheitsverantwortliche auf eine unterstützte Version (9.18, 9.17 oder 9.16) aktualisieren und das jeweils verfügbare RPM Skript nutzen. Alternativ ist es möglich, den Zugriff auf das System Manager Portal (Port 8443) mit einer Firewall-Regel zu unterbinden, um somit nicht mehr aus dem Internet angreifbar zu sein. Mit dem Workaround können auch ältere Produktversionen vor einer Kompromittierung geschützt werden. [IVAN2023c]

Ivanti empfiehlt, den Zugriff auf das System Manager Portal ausschließlich über das interne Netzwerk zu erlauben [IVAN2023b].

Zur Mitigation von CVE-2023-38035 bzw. Ausführung des RPM Skripts muss wie folgt vorgegangen werden [IVAN2023c]:

- Verwenden Sie SSH, um sich über ein Terminal mit einem Administrator-Account 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 "#".
- Installieren Sie nun das RPM-Skript zur Behebung von CVE-2023-38035 mit dem Befehl zu jeweiligen installierten Version:
  - 9.18: *install rpm url https://support.mobileiron.com/ivanti-updates/sentry-security-update-9.18.0-3.noarch.rpm*
  - 9.17: *install rpm url https://support.mobileiron.com/ivanti-updates/sentry-security-update-9.17.0-3.noarch.rpm*
  - 9.16: *install rpm url https://support.mobileiron.com/ivanti-updates/sentry-security-update-9.16.0-3.noarch.rpm*
- Geben Sie *reload* ein, um das System neu zu starten.
- Zur Validierung der vollständigen Installation geben Sie *install rpm info detail mi-mics* ein und stellen Sie sicher, dass die Versionsnummer mit "a" endet (9.18.0a, 9.17.0a, 9.16.0a)

Weitere Informationen zu Mitigationsmaßnahmen finden sich im Knowledge Base Artikel des Herstellers [IVAN2023c].

Links

[IVAN2023a] CVE-2023-38035 - Vulnerability affecting Ivanti Sentry:
https://www.ivanti.com/blog/cve-2023-38035-vulnerability-affecting-ivanti-sentry

[IVAN2023b] CVE-2023-38035 – API Authentication Bypass on Sentry Administrator Interface:
https://forums.ivanti.com/s/article/CVE-2023-38035-API-Authentication-Bypass-on-Sentry-Administrator-Interface

[IVAN2023c] KB API Authentication Bypass on Sentry Administrator Interface - CVE-2023-38035:
https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035

[BSI2023] Zero-Day Schwachstelle in IvantiEndpoint Manager Mobile geschlossen:
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2023/2023-249317-1032.pdf

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