Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Ivanti Cloud Services Appliance – Schwachstellen werden aktiv ausgenutzt

CSW-Nr. 2024-274385-1032, Version 1.0, 20.09.2024

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 19. September 2024 berichtete Ivanti in einem Advisory von beobachteten Angriffen auf Organisationen, die die Lösung "Cloud Services Appliance" (CSA) des Herstellers einsetzen. Demnach würden die Angreifenden zwei kürzlich bekanntgewordene Schwachstellen in CSA kombinieren, um zunächst die Nutzer-Authentifizierung zu umgehen (CVE-2024-8963 – nach dem Common Vulnerability Scoring System (CVSS) in Version 3.0 mit 9.4 als „kritisch“ bewertet [IVAN2024a]) und anschließend Code auf den verwundbaren Geräten auszuführen (CVE-2024-8190 – CVSS-Score: 7.2 / „hoch“ [IVAN2024b]). Obwohl für CVE-2024-8190 bereits am 13. September 2024 Hinweise auf eine aktive Ausnutzung vorlagen, ergaben weitere Analysen nun die Kombination beider Schwachstellen.

Die Attacken seien demnach vereinzelt bei nicht weiter spezifizierten Organisationen beobachtet worden.

Betroffen sind ausschließlich Cloud Services Appliances mit der Software-Version 4.6. Für diese hatte Ivanti den Support mit Sicherheitspatches ursprünglich zum 31. August eingestellt [IVAN2024c], nun jedoch außerplanmäßig doch noch ein Update veröffentlicht.

Ivanti CSA dient dezentral arbeitenden Organisationen unter anderem als Lösung zum sicheren Datenaustausch über das Internet.

* 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

Das betroffene Produkt stellt aufgrund seiner zentralen Rolle zum Zugriff auf organisationsinterne Daten und zur Verwaltung von IT-Systemen ein attraktives Ziel für Cyber-Angriffe dar. Bei einer Kompromittierung könnten vertrauliche Informationen abgegriffen bzw. manipuliert oder weitere Netzwerkkomponenten kompromittiert werden.

Gleichzeitig unterstreicht die Veröffentlichung des Patches – trotz bereits geendetem Sicherheits-Support durch den Hersteller – die Dringlichkeit des Sachverhalts. Die zwischen dem 13. und 19. September gewonnenen Erkenntnisse verschärfen das Bedrohungsszenario deutlich von einer Schadcode-Ausführung mit administrativen Rechten hin zu einer unauthentifizierten Ausnutzung aus der Ferne.

Maßnahmen

Am 10. September hat Ivanti das Sicherheitsupdate 519 für CSA 4.6 herausgegeben, das beide Schwachstellen schließt und von IT-Sicherheitsverantwortlichen daher kurzfristig installiert werden sollte. Gleichzeitig rät der Hersteller aufgrund des auslaufenden Supports der betroffenen Software-Version, zeitnah auf CSA 5.0 zu wechseln.

Um eine eventuell bereits erfolgte Kompromittierung zu detektieren, empfiehlt Ivanti zu prüfen, ob kürzlich Administratoren-Accounts hinzugefügt oder modifiziert wurden. Weiterhin sollten Logs und – falls vorhanden – andere Detektions/Monitoring-Lösungen auf verdächtige Aktivitäten im Zusammenhang mit diesen Nutzerkonten analysiert werden. Sofern hier Angriffe identifiziert werden können, empfiehlt der Hersteller, betroffene Systeme mit CSA 4.6 Patch 519 – oder besser CSA 5.0 – neu aufzusetzen.

Bei weiteren Fragen sollen Betreiber von Ivanti CSA Kontakt zum Support des Unternehmens herstellen [IVAN2024a].

Weitere Hinweise zur sicheren Anbindung von IT-Systemen und zum vertrauensvollen Austausch von Daten über das Internet finden sich an verschiedenen Stellen im IT-Grundschutz des BSI – so z.B. im Baustein "NET.3.3 - VPN" [BSI2024].

Links

[IVAN2024a] Security Advisory Ivanti CSA 4.6 (Cloud Services Appliance) (CVE-2024-8963):
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963

[IVAN2024b] Security Advisory Ivanti Cloud Service Appliance (CSA) (CVE-2024-8190):
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Service-Appliance-CSA-CVE-2024-8190

[IVAN2024c] Ivanti Endpoint Manager and Ivanti Endpoint Manager Security Suite and Ivanti Cloud Service Application (CSA) - End Of Life (EOL):
https://forums.ivanti.com/s/article/Ivanti-Endpoint-Manager-and-Ivanti-Endpoint-Manager-Security-Suite-EOL

[BSI2024] BSI IT-Grundschutz NET.3.3 VPN – Edition 2023:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_3_3_VPN_Edition_2023.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.