Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

Kaseya - IT-Systemhäuser und deren Kunden weltweit durch Supply-Chain-Attacke mit REvil-Ransomware angegriffen

CSW-Nr. 2021-234002-1332, Version 1.3, 12.07.2021

IT-Bedrohungslage*: 3 / Orange

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:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE 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

Kaseya ist ein Anbieter für IT-Management-Lösungen für Managed Service Provider (MSP) bzw. IT-Systemhäuser. Zum Kundenkreis gehören auch viele kleine und mittlere Unternehmen. Zu den Angeboten des Unternehmens zählt die Kaseya VSA Plattform, eine Remote Monitoring und Management (RMM-)Lösung mit der IT-Systemhäuser auf den Systemen ihrer Kunden Dienstleistungen wie Fernwartung, Monitoring, Backup oder Patch-Management durchführen können.

Am Freitag den 2. Juli meldete der Hersteller Kaseya um 22:00 Uhr (MESZ) einen Angriff auf seine Virtual System Administrator (VSA) Software [KAS2021a]. Zur Eindämmung des Angriffes hat der Hersteller alle von ihm betriebenen Software as a Service (SaaS) Systeme bis auf weiteres heruntergefahren [KAS2021b]. Laut Kaseya sind von dem Angriff eine kleine Zahl Kunden (hier konkret IT-Systemhäuser), die Kaseya VSA als On Premise Lösung betreiben, betroffen. Kaseya empfiehlt daher allen Kunden ihre On Premise Syteme sofort herunterzufahren und ausgeschaltet zu lassen.

* 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.

Nach mehreren Medienberichten [BPC2021a] [SPI2021] [DPS2021] handelt es sich bei dem Angriff durch die Ransomwaregruppe REvil. Die Angreifer nutzen ein manipuliertes Update für Kaseya VSA On-Prem-Server, um die Systeme der Opfer mit Ransomware zu attackieren. Dieses Update soll lokale Antiviren-Programme löschen oder unschädlich machen und lokale Dateien über nachgeahmte Windows Defender-Apps verschlüsseln.

Nach aktuellem Kenntnisstand hat die Verschlüsselung der IT-Systemhäuser mit hoher Wahrscheinlichkeit auch Einfluss auf deren Kundensysteme, sodass diese ebenfalls Opfer der Ransomware-Attacke werden. Dabei ist den Kunden der IT-Systemhäuser oftmals nicht bekannt oder bewusst, ob ihre Dienstleister Kaseya Produkte einsetzen, da die IT-Systemhäuser die Systeme unter eigener Marke anbieten können. Kunden können überprüfen, ob Kaseya VSA Systeme zum Einsatz kommen, indem sie prüfen ob unten auf den Webseiten des VSA Systems folgender Schriftzug zu sehen ist: "Powered by Kaseya-Copyright 2000-2008Kaseya. All rights reserved" [KAS2021c].

Nach Angaben von Kaseya sind 40 ihrer Kunden von diesem Angriff betroffen. Diese sind allerdings als IT-Systemhäuser wiederum Dienstleister von teilweise hunderten Unternehmen, so dass die zunächst berichtete Zahl von 200 betroffenen Unternehmen noch weit übertroffen werden kann.

Einzelne Betroffene tauschen sich auf Reddit [Red2021] aus.

Update 1:
Der Infektionsvektor ist weiter unklar. Laut dem Dutch Institute for Vulnerability Disclosure nutzten die Angreifer eine Zero-Day Schwachstelle (CVE-2021-30116) in Kaseya VSA [DIV2021] .

Die Clouddienste von Kaseya sollen im Laufe des 05.07.2021 wieder hochgefahren werden. Für die On-Premise Server will der Hersteller im Laufe des selben Tages Informationen bezüglich Sicherheitspdates auf seiner Webseite veröffentlichen. Bis dahin sollen Kunden die Server deaktiviert lassen.

CISA und FBI haben eine Hilfeseite für betroffene Kunden eingerichtet [DHS2021].

Update 2:
Die Clouddienste von Kaseya sind auch am 9. Juli 2021 noch nicht wieder verfügbar. Betroffene Kunden bleiben aufgefordert auch die On-prem Kaseya-VSA-Systeme weiter deaktiviert zu lassen.

Update 3:
Am 11. Juli wurden Updates für On-Premise-Kunden unter [KAS2021g] bereitgestellt. Mit Stand vom 12. Juli 2021 befinden sich die Cloud-Dienste im Wiederanlauf [KAS2021k]. Laut Hersteller sind ca. 95% aller Kundeninstanzen wieder online.

Bewertung

Bei dem Angriff handelt es sich um einen Supply-Chain-Angriff. Von diesem Angriff können auch Unternehmen betroffen sein, die keine direkte Beziehungen mit dem Unternehmen Kaseya besitzen. Es reicht, wenn ein IT-Systemhaus, bzw. Managed Service Provider (MSP) des Unternehmens Dienste von Kaseya nutzt.

Aufgrund des durch die Angreifer gewählten Zeitpunktes des Angriffs (Freitag Abend), ist aktuell noch von einer möglicherweise hohen Dunkelziffer an Betroffenen auszugehen.

Da nach aktueller Kenntnis die Angreifer eine Schwachstelle in den VSA Systemen ausnutzen, für die bislang kein Patch existiert, sind aktive Systeme weiter der Gefahr einer Verschlüsselung ausgesetzt und sollten deaktiviert werden, beziehungsweise bleiben.

Da alle Kaseya SaaS VSA Systeme abgeschaltet sind, ist aktuell die Verfügbarkeit der Systeme für alle Kunden eingeschränkt, unabhängig davon, ob die Systeme verschlüsselt wurden. Das BSI kann nicht bewerten in wie weit ein Ausfall von Remote Monitoring und Management (RMM-)Systemen wie Kaseya VSA Auswirkungen auf den Betrieb kritischer Geschäftsprozesse hat.

Update 1:
Dem BSI liegen bis jetzt keine belastbaren Informationen zum Infektionsvektor vor. Daher sollten die Hinweise des Herstellers zur Abschaltung, Analyse und zum Wiederanlauf der Systeme beachtet werden [KAS2021a].

Update 2:
Dem BSI liegen Information zu Spam-Mails vor. Im Betreff und Body dieser Nachrichten wird der Sachverhalt aufgegriffen und darauf hingewiesen, dass die im Anhang befindliche ausführbare Datei Abhilfe würde schaffen können. Dabei handelt es sich aber in der Regel um weitere Schadsoftware (z. B. Cobalt Strike) [BPC2021c].

Mögliche Auswirkungen auf Kritische Infrastrukturen inkl. Verwaltung

Der geschilderte Vorfall kann in ähnlicher Art auch Kritische Infrastrukturen treffen und die dargestellten Konsequenzen haben.

In Schweden mussten durch den Angriff am Samstag den 03.07.2021 mehr als 500 Supermärkte des Unternehmens Coop geschlossen bleiben [BPC2021b], da die Kassensysteme aufgrund des Angriffes nicht funktionierten. Dabei war das KRITIS-Unternehmen Coop kein Kunde von Kaseya, aber ihr MSP Visma Esscom.

Maßnahmen

- Aufgrund der zu diesem Zeitpunkt noch unklaren Vorgehensweise der Angreifer, ist es zu empfehlen, auch nicht verschlüsselte Systeme auf eine mögliche Kompromittierung zu überprüfen. Dies ist z.B. mit IoCs aus den unten aufgeführten Links möglich.
- Des Weiteren ist es in diesem Kontext zu empfehlen, vor einer möglichen Wiederherstellung der Systeme geeignete Sicherungsmaßnahmen zum Zwecke einer forensischen Untersuchung vorzunehmen. Aktuell ist unklar ob z.B. auch Daten ausgeleitet werden und ob möglicherweise auch weitere Malware wie Backdoors Verwendung finden. Eine forensische Analyse könnte möglicherweise Hinweise darauf geben.
- Unternehmen, deren IT-Systemhaus Kaseya Produkte einsetzen sollten sich umgehend mit ihrem Dienstleister in Verbindung setzen. Betroffene IT-Systemhäuser sollten sich direkt an Kaseya wenden und den Maßnahmenempfehlungen des Hersteller folgen [KAS2021a]. Hierzu zählt insbesondere auch, dass alle selbst betriebenen Kaseya VSA Systeme unverzüglich abgeschaltet werden, beziehungsweise bis auf weiteres abgeschaltet bleiben sollten.
- Unternehmen, die erst nach dem Wochenende eine Betroffenheit feststellen, sollten Systeme die am Wochenende ausgeschaltet waren, weiter ausgeschaltet lassen um die eine Verschlüsselung dieser Systeme zu verhindern.

Update 1:

- Der Hersteller bietet ein Analysetool zum Download an, das VSA Server und verwaltete Endpunkte auf eine Kompromittierung prüfen kann [KAS2021d].
- Vom Angreifer hinterlegte Links könnten laut Angabe von Kaseya zu schadhaften Exploit-Webseiten führen [KAS2021a] und sollten nicht ohne Schutzmaßnahmen aufgerufen werden.
- Einige AV-Programme entfernen bei einer Bereinigung nicht nur die Ransomware, sondern auch Konfigurationsdateien, in den Teile des Verschlüsselungs-Keys gespeichert sind. Falls eine Entschlüsselung notwendig werden sollte, müssen diese Konfigurationsdateien vorher gesichert werden.

Update 2:

- Entgegen der früheren Ankündigungen des Herstellers steht zum heutigen Zeitpunkt weiterhin noch kein Update zur Verfügung. Nach derzeitigem Stand soll dieses am Sonntag, den 11. Juli 2021 ab 20:00 Uhr veröffentlicht werden. Betroffene Kunden sollen vor der Installation die durch Kaseya zur Verfügung gestellten aktualisierten Werkzeuge zur Detektion [KAS2021f] ausführen und zusätzlich ein so genanntes Runbook befolgen [KAS2021e].
- Um eventuelle weiteren Auffälligkeiten feststellen zu können, sollten nach der Installation der Updates die folgenden Mindestmaßnahmen zwecks Logging etabliert werden:
  - Firewall-Logging Richtung VSA und vom VSA ausgehend erhöhen.
  - Powershell-Logging auf VSA-Server erhöhen.
  - Zentralisiertes Event-Logging für VSA-Server und DC.
  - Zentralisiertes IIS-Log für VSA-Server.

› Nach Möglichkeit sollten die zentralen Log-Server separaten Rechtedomänen unterliegen und von den übrigen Systemen maximal abgeschirmt sein.

Update 3:

- Der Hersteller hat am 11.07.2021 Upates für On-Premise-Kunden unter [KAS2021g] zur Installation bereitgestellt.
- Kaseya weist ausdrücklich darauf hin, dass die Anweisungen zum Wiederanlauf unter [KAS2021e] sowie die Härtungsmaßnahmen und Best Practices unter [KAS2021h] für On-Premise-Kunden vor der Installation des neuen Releases befolgt werden sollten.
- Für SaaS-Kunden wurden unter [KAS2021i] Anweisungen für den Wiederanlauf sowie Best Practices unter [KAS2021k] veröffentlicht.

Indicators of Compromise

Die in den folgenden Quellen enthaltenen IoCs stammen aus einer OSINT-Recherche und wurde durch das BSI nicht im einzelnen geprüft.

- Malware Information Sharing Platform - MISP-Event "Kaseya Supply Chain attack with REvil ransomware" UUID: c94ba584-d07a-4a3c-82c0-61d5abede7a2 (Hashes, Dateinamen, C2-Domains, Yara-Regeln)
- Kaseya VSA Supply-Chain Ransomware Attack https://community.sophos.com/b/security-blog/posts/active-ransomware-attack-on-kaseya-customers
- Kaseya IoCs - https://docs.google.com/spreadsheets/d/11AFPdK5A-7g484lfc0HmXdBrZpYI-Jhx4N1VwFXrcrQ/edit?usp=sharing
- Yara Regel - https://github.com/Neo23x0/signature-base/blob/master/yara/crime_revil_general.yar
- Resources for DFIR Professionals Responding to the REvil Ransomware Kaseya Supply Chain Attack https://www.cadosecurity.com/post/resources-for-dfir-professionals-responding-to-the-revil-ransomware-kaseya-supply-chain-attack
- https://github.com/cado-security/DFIR_Resources_REvil_Kaseya

Fragen an IT-Sicherheitsverantwortliche

- Setzen Sie oder einer ihrer Dienstleister Kaseya VSA Systeme ein?
- Falls ja, wurden Sie zu dem Vorfall informiert? Falls nein, sollten Sie die Meldewege zu diesem Dienstleister prüfen.
- Sind die Handlungsanweisungen des BSI [BSI2021a] zur Reaktion auf Ransomware-Vorfälle bekannt?
- Sind die allgemeinen Handlungsanweisungen des BSI [BSI2021b] zur Reaktion auf einen IT-Sicherheitsvorfall bekannt?
- Falls Sie betroffen sind, wurde der Vorfall schon über die etablierten Kanäle an das BSI gemeldet?
- Besteht ein Anschluss an einen Malware Information Sharing Portal (MISP) Verbund, sodass die Informationen des MISP-Events "Kaseya Supply Chain attack with REvil ransomware" UUID: c94ba584-d07a-4a3c-82c0-61d5abede7a2 genutzt werden können?

Update 1:

- Nutzen Sie Multi-Faktor-Authentifizierung zur Anmeldung an ihren RMM und Admin Systemen?
- Werden die RMM Systeme in einem getrennten Managementment-Netz betrieben, auf welches nur über ein VPN von außen zugegriffen werden kann?

Update 2:

- Betroffene Dienstleister, welche verschiedene Dienste aggregieren, sollten die BSI-Empfehlungen für den sicheren Einsatz von Application Delivery Controllern beachten [BSI2021c].

Links

[KAS2021a] - Kaseya - Updates Regarding VSA Securiy Incident
https://www.kaseya.com/potential-attack-on-kaseya-vsa/

[KAS2021b] - Kaseya Cloud Status
https://status.kaseya.net/pages/maintenance/5a317d8a2e604604d65c1c76/60df588ba49d1e05371e9d8b

[KAS2021c] - Kaseya - How do I white label the Kaseya software so that my customers are not aware that I am using Kaseya to provide services to them?
https://helpdesk.kaseya.com/hc/en-gb/articles/229037308-How-do-I-white-label-the-Kaseya-software-so-that-my-customers-are-not-aware-that-I-am-using-Kaseya-to-provide-services-to-them-

[KAS2021d] - Kaseya VSA Detection Tool
https://kaseya.app.box.com/s/0ysvgss7w48nxh8k1xt7fqhbcjxhas40

[KAS2021e] - On Premises VSA Startup Readiness Guide
https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993

[KAS2021f] - Kaseya VSA Detection Tool
https://kaseya.app.box.com/s/p9b712dcwfsnhuq2jmx31ibsuef6xict

[KAS2021g] - 9.5.7a Feature Release - 11 July 2021
https://helpdesk.kaseya.com/hc/en-gb/articles/4403785889041-9-5-7a-9-5-7-2994-Feature-Release-11-July-2021-

[KAS2021h] - VSA On-Premises Hardening and Best Practice Guide
https://helpdesk.kaseya.com/hc/en-gb/articles/4403760102417

[KAS2021i] - VSA SaaS Startup Guide - July 7, 2021
https://helpdesk.kaseya.com/hc/en-gb/articles/4403709476369

[KAS2021j] - VSA SaaS Best Practices
https://helpdesk.kaseya.com/hc/en-gb/articles/4403622421009-VSA-SaaS-Best-Practices

[KAS2021k] - Important Notice July 12th, 2021
https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-12th-2021

[BPC2021a] - REvil ransomware hits 200 companies in MSP supply-chain attack
https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-200-companies-in-msp-supply-chain-attack/

[BPC2021b] - Coop supermarket closes 500 stores after Kaseya ransomware attack
https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/

[SPI2021] - Cyberangriffe auf Supermarktkette Coop und IT-Dienstleister
https://www.spiegel.de/netzwelt/coop-und-kaseya-mehrere-firmen-von-hackerangriffen-betroffen-a-4bdcf7a5-87e5-45a7-b69d-c14a605e0f8d

[BSI2021a] - Ransomware: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.1:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf

[BSI2021b] - Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen_node.html

[BSI2021c] - Empfehlungen für den sicheren Einsatz von Application Delivery Controllern
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Hilfsmittel_Empfehlung_ApplicationDeliveryController_v1.html

[Git2021] - Resources for DFIR Professionals Responding to the REvil Ransomware Kaseya Supply Chain Attack
https://github.com/cado-security/DFIR_Resources_REvil_Kaseya

[Red2021] -Crticial Ransomware Incident in Progress
https://www.reddit.com/r/msp/comments/ocggbv/crticial_ransomware_incident_in_progress/

[DPS2021] - Kaseya supply chain attack delivers mass ransomware event to US companies

https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b

[DIV2021] - Kaseya Case Update 2
https://csirt.divd.nl/2021/07/04/Kaseya-Case-Update-2/

[DHS2021] - CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack
https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

[BPC2021c] - Fake Kaseya VSA security update backdoors networks with Cobalt Strike
https://www.bleepingcomputer.com/news/security/fake-kaseya-vsa-security-update-backdoors-networks-with-cobalt-strike/

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 TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. 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. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

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:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.