Landespolizeipräsidium · Mainzer Straße 134-146. ·66121 Saarbrücken

Landespolizeipräsidium
LPP 2 Kriminalitätsbekämpfung/
Landeskriminalamt

Dezernat LPP 222

Dienst-gebäude: Hellwigstraße 8-10
66121 Saarbrücken

Bearbeiter_in: Schmitt M.O.KHK
Tel.: 0681 962 – 2431
Fax: 0681 962 –2445
E-Mail: cybercrime@polizei.slpol.de

Az: 26/2021

Datum: 05.07.2021

Information der
Zentralen Ansprechstelle Cybercrime (ZAC) des Landespolizeipräsidiums Saarland

Warnmeldung der zentralen Ansprechstelle Cybercrime (ZAC) Saarland hinsichtlich des Supply Chain Angriffs (Revil) auf Produkte der Firmen Kaseye, Visma Esscom

Bei Kaseya handelt es sich um einen 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.

Visma Esscom ist ein Zahlungsdienstleister der Produkte von Kaseya einsetzt.
Produkte von Visma Esscom werden vor allem von Klein und Mittelständischen Unternehmen eingesetzt.

Weil der Zahlungsdiensleister Visma Esscom Opfer einer Hacker-Attacke wurde, musste die schwedische Coop-Supermarktkette hunderte Läden schließen. Der Grund dafür sind nicht mehr funktionierende Kassensysteme. Die Schwedische Supermarktkette schloss zeitweise alle 800 Filialen.

Der US IT-Dienstleister Kaseya mit 36.000 Kunden wurde am 02.07.2021 mutmaßliches Ziel eines Cyberangriffs durch Ransomware Revil. Kaseya verwaltet mit dem Fernzugriffs- und Wartungssoftware VSA Softwareupdates auf IT-Systemen. Weiteres Opfer des Cyberangriffs ist Zahlungsdienstleister Visma Esscom (1 Mio Kunden) mit negativen Auswirkungen auf das Kassensystem von Coop.

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

Die Polizei rät:

- 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 Dienstleisterprüfen.

- Sind die Handlungsanweisungen des BSI [BSI2021a] zur Reaktion auf Ransomware-Vorfälle bekannt?

- Sind die allgemeinen Handlungsanweisungen des BSI [BSI2021b] zur Reaktion auf einen IT-Sicherheitsvorfallbekannt?

- Falls Sie Betroffener der Ransomwarekampagne sind, haben Sie den Vorfall schon gemeldet (Polizei/BSI)?

- Im Falle der Betroffenheit >> Erstatten Sie Anzeige.

Maßnahmen

- Aufgrund der zu diesem Zeitpunkt noch unklaren Vorgehensweise der Angreifer, ist es zu empfehlen, auch nichtverschlüsselte Systeme auf eine mögliche Kompromittierung zu überprüfen.

  Dies ist z.B. mit IoCs aus den nachfolgend 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 Herstellers folgen. Hierzu zählt insbesondere auch, dass alle selbst betriebenen Kaseya VSA Systeme unverzüglich abgeschaltet werden, beziehungsweise bis auf weiteres abgeschaltet bleiben sollten.

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

Polizei

SAARLAND

Quellen:

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

- [KAS2021b] - Kaseya Cloud
  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 usingKaseya 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-

- [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

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

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

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

- [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

Mit freundlichen Grüßen,

i.A.
KHK M.O. Schmitt
Zentrale Ansprechstelle
Cybercrime Saarland

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken