AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Kaseya VSA Supply-Chain Ransomware Attack

(CVE-2021-30116)

06/07/2021

Autoriteti Kombëtar për Certifikim Eletronik dhe Sigurinë Kibernetike
Rruga. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Shqipëri 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

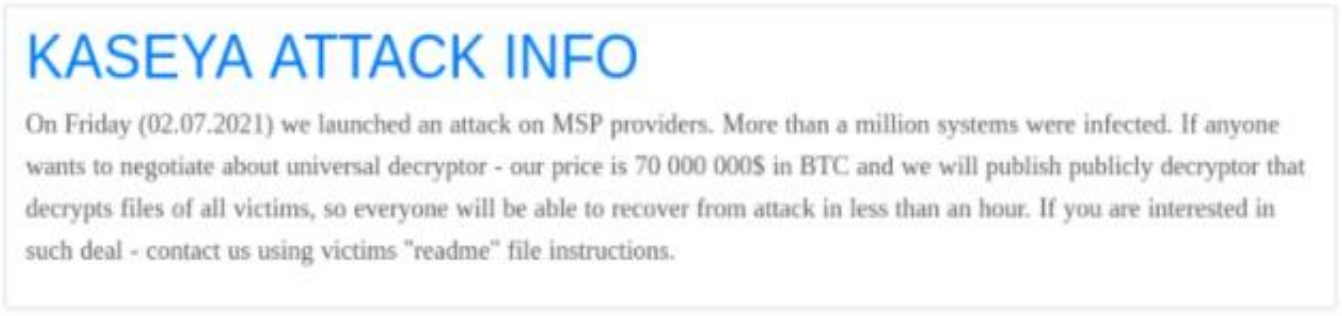
Indeksi

Përmbledhje CVE-2021-30116.....3
Rekomandime për MSP-të e prekura.....5
Rekomandime për klientët e prekur.....5
Referenca dhe burime: 6

Përmbledhje CVE-2021-30116

Dobësitë e shumëfishta “Zero-Days” në Kaseya VSA shfrytëzohen për të shpërndarë Ransomware Revil.

Akcesk ju informon rreth një sulmi që ka impaktuar kompaninë Kaseya.



Janë bërë shumë raportime nga një numër i konsiderueshëm i kompanive, rrjetet e të cilave administrohen nga ofruesit e shërbimeve të menaxhuara (Managed Service Providers) duke përdorur Kaseya Virtual System Administrator (VSA), një program monitorimi dhe menaxhimi në distancë (Remote Managed Monitoring) nga Kaseya Limited. Këto kompani që përdornin këto sisteme u bënë viktima të një sulmi “Ransomware”. Sulmi është shpërndarë gjeografikisht në çdo klienti kësaj kompanie. Numri i kompanive të impaktuara deri tani janë afërsisht 800-1500. Kaseya Limited ka deklaruar se sulmi filloi rreth orës 14:00 / 18:00 të Premten, 2 korrik 2021, ku dëmi financiar përllogaritej rreth 70 000 000 $ për tu konvertuar në BitCoin dhe ata po janë akoma duke investiguar për më shumë detaje rreth këtij incidenti.

Sulmet i përkasin “Ransomware” REvil[1], i njohur gjithashtu si (Sodinokibi), një nga grupet më aktive të Ransomware. REvil operon si Ransomware-as-a-Service (RaaS), përmes së cilës zhvillojnë vetë ngarkesën e Ransomware dhe sigurojnë infrastrukturën për menaxhimin e komunikimeve të viktimave për negocimin e pagesës dhe shpërndarjen e mjeteve të dekriptimit të pajisjeve dhe sistemeve të kompanive “viktimë” të cilat janë afektuar.

Duket se sulmuesit kanë përdorur një dobësi “Zero-Day” për të patur akses në distancë në serverët VSA të Kaseya-s. Duke qënë që Kaseya përdoret kryesisht nga Ofruesit e Shërbimeve të Menaxhuara (MSPs), kjo qasje u dha sulmuesve një akses të privilegjuar në pajisjet e klientëve të MSP. Disa nga funksionalitetet e një serveri VSA janë: vendosja e softuerit dhe automatizimi i detyrave të IT-së. Si i tillë, ai disponon një nivel të lartë besimi në pajisjet e klientit, e cila jep mundësinë të infiltrohen në serverët e VSA në çdo klient, të cilin e detyrojnë të kryejë çfarëdo detyre që kërkon ky server. Kjo është një nga arsyet pse Kaseya u vu në shënjestër. Për fat të keq, REvil i shfrytëzoi dobësitë para se klientët të mund të përditësoheshin.

[2]CISA (Cybersecurity and Infrastructure Security Agency) dhe FBI (Federal Bureau of Investigation) vazhdojnë t'i përgjigjen sulmit të Ransomware duke shfrytëzuar një dobësi në softuerin Kaseya VSA kundër ofruesve të shërbimit të menaxhuar (MSP) dhe klientëve të tyre.

MSP-të e prekura dhe klientët e tyre duhet të ndjekin udhëzimet më poshtë:

[1] https://en.wikipedia.org/wiki/REvil

[2] https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

Rekomandime për MSP-të e prekura

- [3]Shkarkoni mjetin e dekriptimit Kaseya VSA. Ky mjet analizon një sistem dhe përcakton nëse ka indikatorë të ndërhyrjes së mundshme në sistem apo rrjet.
- Aktivizoni autentikimin (MFA multi-factor authentication) në secilën llogari që është nën kontrollin e organizatës apo kompanisë suaj.
- Implementoni një listë që lejon komunikimin me RMM (Remote Monitoring and Management) me IP-të të aprovuara.
- Vendosni ndërfaqet administrative të RMM në një VPN ose një Firewall në një rrjet të dedikuar administrativ.

Rekomandime për klientët e prekur

- Sigurohuni që të bëni back-up të vazhdueshëm të sistemit tuaj.
- Aplikoni një proces manual të menaxhimit të përditësimeve, përfshi instalimin e "patcheve" sapo ato të jenë të disponueshme.
- Implementoni MFA dhe parimin e privilegjeve më të pakta (Principle of Least Privilege) në llogaritë e administratorëve.
- Përdorimi i një antivirusi të licencë dhe Endpoint Data Protection (EDP).

Për më shumë info:

Rast simulimi konkret i Revil ransomware.

https://twitter.com/SophosLabs/status/1412056467201462276?s=20

[3] https://kaseya.app.box.com/s/0ysvgss7w48nxh8k1xt7fqhbcjxhas40

Referenca dhe burime:

https://www.youtube.com/watch?v=IJTMkyhLIoQ&ab_channel=LawrenceSystems

https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116

https://community.sophos.com/b/security-blog/posts/active-ransomware-attack-on-kaseya-customers

https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-6th-2021

https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details

https://kaseya.app.box.com/s/0ysvgss7w48nxh8k1xt7fqhbcjxhas40

https://www.cyberscoop.com/us-biden-ransomware-revil-kaseya/

https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

https://us-cert.cisa.gov/ncas/current-activity/2021/07/02/kaseya-vsa-supply-chain-ransomware-attack