TLP:WHITE

SUNDHEDSDATA-
STYRELSEN

Cybervejrudsigt i sundhedssektoren

Q4 2021

Publiceret af:
Den decentrale cyber- og informationssikkerhedsenhed i sundhedssektoren (DCISSund)

DCISsund@sundhedsdata.dk

@DCIS_Sund

Introduktion

Baggrund

Cybervejrudsigten publiceres af sundhedssektorens DCIS (Decentral cyber- og informationssikkerheds-enhed) hvert kvartal og er en opdatering på de vigtigste aktuelle cyber- og informationssikkerheds-hændelser i sundhedssektoren.

Cybervejrudsigten skaber et overblik over begi-venheder fra de seneste kvartaler og forudsiger på baggrund af disse, hvilke begivenheder, der kan forventes i det næste kvartal.

Den kan benyttes som sektorspecifik rådgivning til sundhedssektorens løbende risikovurdering og ope-rative overblik.

Datagrundlag

DCIS overvåger og udsender løbende varsler til aktører i sundhedssektoren. Varslerne udsendes på baggrund af data fra vores kollegaer i sundhedssek-toren globalt set. Disse triagerer vi med information fra Center for Cybersikkerhed (CfCS), risikovurderin-ger fra aktørerne i sektoren, åbne kilder samt andre sektor-DCIS'er.

De oplistede varsler er et udpluk af de mest kritiske udsendte varsler. Listerne er derved ikke udtømmende.

TLP-mærkning

Al information, som sendes ud fra sundhedssekto-rens DCIS, TLP-mærkes.

TLP-skalaen er opdelt i fire niveauer, som både i navn og farvekode indikerer, hvor følsomme informa-tionerne er, og hvordan de må anvendes af modtage-ren. Det er vigtigt at understrege, at restriktionerne for deling både gælder det markerede dokument samt anden mundtlig og skriftlig omtale af indholdet.

TLP:WHITE - Informationerne anses ikke som sær-ligt følsomme og kan frit deles. WHITE vælges, når afsenderen har vurderet, at der er minimal eller slet ingen risiko ved at offentliggøre informationerne.

Kritikalitet

DCIS har valgt at benytte samme metodik som CIS (Center for Internet Security) til vurdering af trus-selsniveau.

Truslen vurderes inden for 5 niveauer og afbildes med 5 ikoner og farver, som ses nedenfor.

Lav:Grøn | Generel:Blå | Øget:Gul | Høj:Orange | Kritisk:Rød

SUNDHEDSDATA-STYRELSEN

Resume

DCIS løftede i december trusselniveauet til Øget:Gul, hvilket betyder, at det er vurderes, at der er en bety-delig risiko for hacking, malware eller anden ondsin-det aktivitet, der kan lede til alvorlig tab af tilgæn-gelighed, fortrolighed, autenticitet eller integritet på tværs af flere kritiske samfundsydelser.

På dette niveau er der kendte sårbarheder, der bliver udnyttet, og udfaldet vurderes at have moderate konsekvenser.

Alternativt er der sårbarheder, der kunne blive udnyttet til at foretage alvorlig skade eller forstyr-relse.

Log4Shell-sårbarhederne er en af de drivende fak-tore til at trusselsniveauet blev øget fra Generel:Blå til Øget:Gul

Log4Shell

DCIS var i forbindelse med Log4Shell sårbarheden i Niveau 1 Informationsberedskab: *Varsling af DCIS og nøglefunktioner ved operatører af væsentlige tjenester inden for sundhedssektoren med henblik på skærpet overvågning.* Niveau 1 kan aktiveres ved henvendelse fra operatører af væsentlige tjenester inden for sundhedssektoren samt Center for Cyber-sikkerhed.

Informationsberedskab kan fx etableres ved efter-retninger om, at det er overvejende sandsynligt, at operatører af væsentlige tjenester i sundhedssekto-ren vil rammes af malware eller er mål for ondsin-dede aktører. Det kan også aktiveres på baggrund af mindre lokale hændelser, hvor der er en mistanke om, at årsagen er malware eller ondsindede aktører.

DCIS trådte ud af informationsberedskab medio december men følger stadig situationen nøje og er i tæt dialog med aktører i sundhedssektoren.

Det forventes at Log4Shell-sårbarhederne vil være aktuelle i lang tid grundet udbredelsen, integrationen i infrastrukturen og den simple angrebsvektor.

Malware

Den frygtede Emotet malware er begyndt at røre på sig igen. Dette til trods for et internationalt samar-bejde i Europol med at få taget malwaren ned.

Emotet åbner døre til Information stealers, Trojans og Ransomware. Trikbot, QakBot og Ryuk er nok de mest kendte malware som benytter Emotet til sine exploids.

#Emotet #BazarLoader #Solarmarker #Zloader #Dridex

DDoS

Der observeres Distributet Denial of Service (DDoS) angreb bredt i sundhedssektoren, truslen gælder internationalt, såvel som nationalt.

Ransomware

Truslen vedrørende ransomware er fortsat aktuel, og særligt i forbindelse med Log4Shell-sårbarhederne frygtes det, at sårbarheden udnyttes til at inficere sårbare systemer med ransomware.

Anbefalinger:

DCIS anbefaler, at man aktivt søger og udbedrer Log4Shell-sårbarhederne. Derudover bør man generelt overveje at:

- Identificer sårbare systemer
- Øge overvågning af kritiske systemer
- Implementere passende modforanstaltninger for at beskytte sårbare kritiske systemer
- Teste og implementere så hurtigt som muligt, når løsninger fx patchs er tilgængelige.
- Opretholde offline backups af kritiske data for at beskytte mod tab af integritet eller tilgængelighed i tilfælde af brud.

Nuværende trusselsniveau: Øget:Gul

SUNDHEDSDATA-
STYRELSEN

Varsler & hændelser i sundhedssektoren

1. Kvartal 2021

Øget

Udvalgte varsler

- Bagdør i Zyxel enheder
- Citrix DDOS
- Sårbarheder i Cisco udstyr

Antal udsendte varsler

2. Kvartal 2021

Generel

Udvalgte varsler

- DNS sårbarheder
- FluBot smishing
- Sårbarhed i Kerberos

Antal udsendte varsler

3. Kvartal 2021

Generel

Udvalgte varsler

- Kritisk sårbarhed i FortiWeb OS
- Aktiv udnyttelse af ProxyShell sårbarheder
- Sårbarheder i Atlassain Confluence
- Sårbarheder i Palo Alto produkter

Antal udsendte varsler

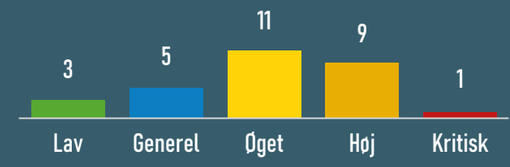
4. Kvartal 2021

Øget

Udvalgte varsler

- Kritisk sårbarhed i Apache Log4j kodebibliotek
- Citrix ADC, Citrix Gateway og Citrix SD-WAN WANOP
- Zero-day i Windows installer (MSI)
- Multiple Vulnerabilities in Apache HTTP Server Affecting Cisco Products

Antal udsendte varsler



SUNDHEDSDATA-
STYRELSEN

Varsler & hændelser 2021 Q4

Kritisk sårbarhed i Apache Log4j kodebibliotek

10. december 2021 - Øget:Gul

Apache Software Foundation har udgivet en sikkerhedsadvisering for at løse en sårbarhed ved fjernudførelse af kode (CVE-2021-44228), der påvirker Log4j version 2.0-beta9 til 2.14.1.

En fjernangriber kan udnytte denne sårbarhed til at tage kontrol over et berørt system. Log4j er et open source, Java-baseret logningsværktøj, der er meget brugt af virksomhedsapplikationer og cloud-tjenester.

DCIS opfordrer brugere og administratorer til at gennemgå Apache Log4j 2.15.0-meddelelsen og opgradere til Log4j 2.15.0 eller anvende de anbefalede begrænsninger med det samme.

11. december 2021 - Høj:Orange

Apache Log4j er et bredt anvendt kodebibliotek, der er designet til at forenkle logning, særligt i Java baserede applikationer.

Ifølge Apache er der d. 9. december blevet opdaget en kritisk sårbarhed i kodebiblioteket, som kan føre til fjernafvikling af arbitrær kode, såkaldt "Remote Code Execution". Sårbarheden bliver sporet under CVE-2021-44228, og har ifølge Apache en CVSS score på 10.0, dvs. højeste kritikalitet. Sårbarheden bliver også omtalt som "Log4Shell".

Flere åbne kilder har rapporteret, at sårbarheden allerede bliver set udnyttet, og forsøgt udnyttet, af ondsindede aktører.

Anbefaling: Center for Cybersikkerhed anbefaler at egenudviklede it-løsninger, der anvender Log4j kodebiblioteket i en udgave mellem version 2.0-beta9 og 2.14.1 opdateres til nyeste version, 2.15.0. I version 2.15.0 er konfigurationen, der muliggør sårbarheden slået fra i bibliotekets standardkonfiguration.

Center for Cybersikkerhed anbefaler, at anvendelsen af biblioteket undersøges uanset version. Hvis det ikke er muligt at opdatere til en nyere version af biblioteket har Apache udgivet en række konfigurationsændringer, der kan forhindre udnyttelsen af sårbarheden.

14. december 2021 - Kritisk:Rød

Set i lyset af de seneste dages udvikling har DCIS valgt at forhøje tidligere udsendte varsel til 'rød' (højeste niveau)

Pga. udbredelsen af log4j generelt og i sundhedssektoren, samt den tunge proces i at finde og patche systemer

Via åbne kilder ser vi bred udnyttelse af sårbarheden, hvor indikationer af feks. cryptominers, malware (Mirai og Muhstik botnets (DDoS)), Cobalt strike tools (muligt ransomware) er tilstede.

OBS: Applikationer, hvor log4j er embedded i installation, skal I være særligt opmærksomme på, at den sårbare version ikke installerer igen, eller opdateres

Kan dette ikke lade sig gøre, bør man eksempelvis benytte

Environment='JAVA_OPTS="-Dlog4j2.formatMsgNoLookups=true" "-Xmx4g'

I bør desuden få tjekket logs i jeres firewalls, om der har været forbindelser mod log4j services fra primo december, da vi er blevet oplyst om, at der har udnyttelse allerede herfra.

Kilde:

https://logging.apache.org/log4j/2.x/security.html

Zero-day i Windows installer (MSI)

29. november 2021 - Høj:Orange

Hackere er begyndt at udnytte zero-day sårbarhed i Windows installer (MSI)

ALLE Windows versioner har denne Zero-day

Det anbefales at opsætte særlige firewall regler for at mitigere sårbarheden.

Kilde:

https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/hackers-exploiting-zero-day/?amp

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41379

Citrix ADC, Citrix Gateway og Citrix SD-WAN WANOP

10. november 2021 - Høj:Orange

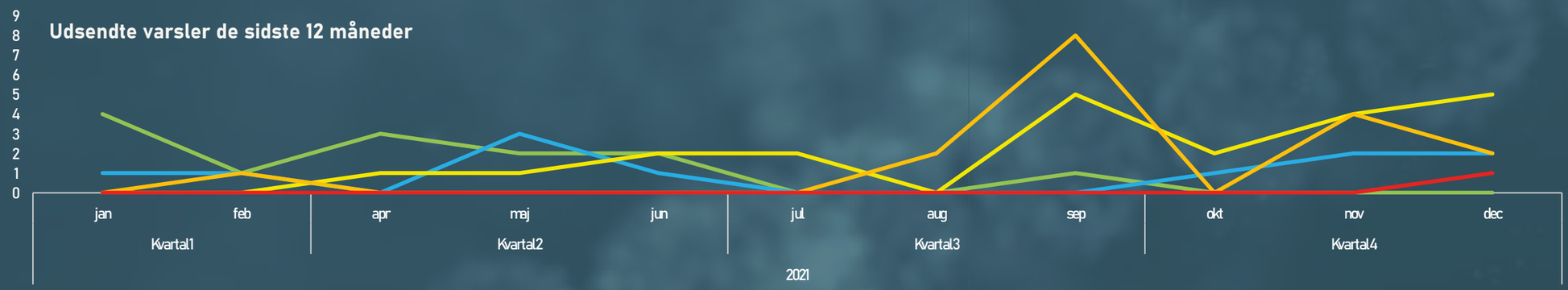
Der er blevet identificeret sårbarheder i Citrix ADC (tidl. NetScaler ADC), Citrix Gateway (tidl. NetScaler Gateway) og Citrix SD-WAN WANOP appliance modeller: 4000-WO, 4100-WO, 5000-WO, 5100-WO.

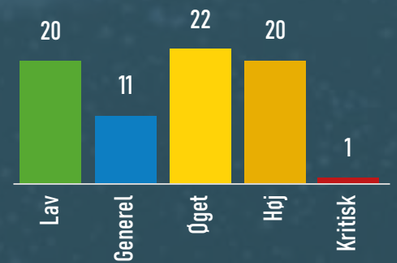
Citrix anbefaler kraftigt, at man installerer den relevante opdatering med det samme. Derudover skal man, efter opgradering redigere konfigurationen for at afhjælpe CVE-2021-22956.

Kilde:

https://support.citrix.com/article/CTX330728

https://support.citrix.com/article/CTX331588





SUNDHEDSDATA-
STYRELSEN

DCISSund

Den decentrale cyber- og informationssikkerhedsenhed for sundhedssektoren

Den decentrale cyber- og informationssikkerhedsenhed i sundhedssektoren (DCISSund) skal styrke arbejdet med cyber- og informationssikkerhed på tværs af den danske sundhedssektor.

Læs mere om DCISSund her