Sundhedsudvalget 2021-22
SUU Alm.del - Bilag 469
Offentligt

TLP:WHITE

SUNDHEDSDATA-
STYRELSEN

Cybervejrudsigt i sundhedssektoren

Q2 2022

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

DCISsund@sundhedsdata.dk

@DCIS_Sund

Introduktion

Baggrund

Cybervejrudsigten publiceres af sundhedssektorens DCISsund (Decentral cyber- og informationssikkerhedsenhed) hvert kvartal og er en opdatering på de vigtigste aktuelle cyber- og informationssikkerhedshændelser i sundhedssektoren.

Cybervejrudsigten skaber et overblik over begivenheder 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 operative overblik.

TLP-mærkning

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

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

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

Datagrundlag

DCISsund overvåger og udsender løbende varsler til aktører i sundhedssektoren. Varslerne udsendes på baggrund af data fra vores kollegaer i sundhedssektoren globalt set. Disse triagerer vi med information fra Center for Cybersikkerhed (CfCS), risikovurderinger 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.

Kritikalitet

DCISsund har valgt at benytte samme metodik som CIS (Center for Internet Security) til vurdering af trusselsniveau.

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

DCISsund sænker trusselsniveauet til Generel:Blå, hvilket indikerer en generel risiko for hacking, malware eller anden ondsindet aktivitet, der kan lede til alvorlig tab af tilgængelighed, fortrolighed, autenticitet eller integritet.

Det vurderes, at der er et potentiale for ondsindede cyberaktiviteter, men der er ikke eksempler på igangværende udnyttelse.

Nets nedbrud

Den 21. juni 2022 blev Nets ramt af et nedbrud.

Valideringen af brugere gennem det såkaldte rod-certifikat (ICA3) var berørt af den aktuelle driftsforstyrrelse. Dette certifikat benyttes til validering af omkring en tredjedel af brugerne af NemID.

En del systemer i sundhedssektoren var ramt af nedbruddet, DCISsund gik derfor i et let informationsberedskab, for at sikre hurtig og effektiv dialog med sundhedssektorens aktører.

DCISsund fulgte og undersøgte situationen nøje og var i tæt dialog med berørte aktører. Der blev varslet om hændelsen bredt i sektoren.

Nets foretog en teknisk ændring d. 26. juni hvilket fik systemerne tilbage på normal drift, hvorefter DCISsund gik ud af informationsberedskabet.

Krigen i Ukraine

Siden krigen i Ukraine startede, har DCISsund arbejdet på robusthed i sektoren. Der blev skruet yderligere op for videndelings niveauet på tværs af landet, med ugentlige møder, sammen med regioner og kommuner, hvor robushed og trusler blive vurderet.

DCISsund udarbejder derudover ugentlige briefs, som indeholder det aktuelle situationsoverblik, trusselsbillede, status i sektoren, anbefalinger, risikoscenarier og ad-hoc vurderinger, som løbende sendes ud til sektoren.

Indtil videre har Rusland primært angrebet kritisk infrastruktur inden for finans- og telesektoren samt statslige hjemmesider i Ukraine. Vi formoder, at dette også vil være gældende, hvis Rusland vælger at angribe allierede til Ukraine.

Der advares i bredt omkring "collateral damage", hvis man benytter Ukrainske leverandører. "Collateral damage" dækker over hændelser og/eller skader, som ikke kun har konsekvenser for det tilsigtede/direkte mål.

Anbefalinger:

DCISsund anbefaler, at man sikrer at beredskabsplaner og backups er opdaterede og tilgængelige, og stadig aktivt søger og udbedrer Log4Shell-sårbarhederne.

På nuværende trusselsniveau Generel:Blå bør man generelt overveje at:

- Identificer sårbare systemer
- Øge overvågning af kritiske systemer
- Implementere passende modforanstaltninger for at beskytte sårbare kritiske systemer
- Når løsninger, fx patches er tilgængelige, test og implementer i et vindue, der passer driften

Derudover bør man i stadig relation til trusselsbilledet i forbindelse med krigen i Ukraine:

- Sikrer sig, at beredskabsplaner er opdaterede og tilgængelige.
- Opretholde offline backups af kritiske data for at beskytte mod tab af integritet eller tilgængelighed i tilfælde af brud.
- Øget awareness til medarbejderes omkring mulige phishing-angreb.

SUNDHEDSDATA-
STYRELSEN

Varsler & hændelser i sundhedssektoren

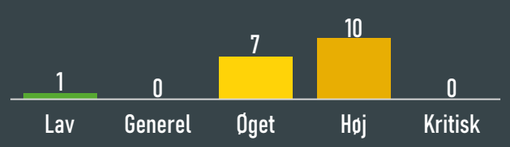
3. Kvartal 2021

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



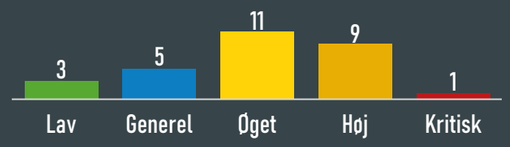
4. Kvartal 2021

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



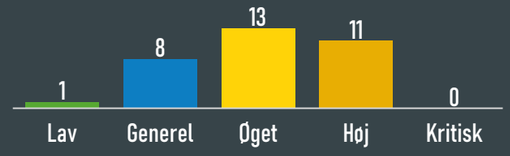
1. Kvartal 2022

Øget

Udvalgte varsler

- Destruktive cyberangreb observeret mod ukrainske organisationer
- Zero-day fix til apple enheder
- Zero-day i Google Chrome browser
- Øget fokus på kritisk infrastruktur
- 2 Zero-days i Mozilla Firefox
- Sårbarhed i Infusionspumper

Antal udsendte varsler



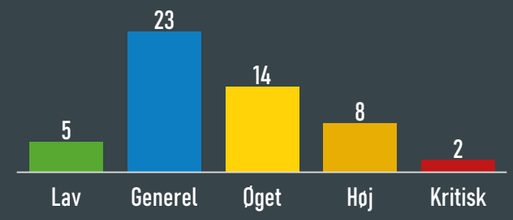
2. Kvartal 2022

Generel

Udvalgte varsler

- Kritiske sårbarheder i VMware
- Kritisk opdatering til Zyxel firewlls og VPN
- TLSstorm sårbarhed i Avaya og Aruba
- Hackere udnytter kritisk fejl i Zyxel firewalls og VPN'er
- Alvorlige sårbarheder i SonicWall SSLVPN SMA 1000-serien

Antal udsendte varsler



SUNDHEDSDATA-
STYRELSEN

Varsler & hændelser Q2 2022

Kritisk opdatering til Zyxel firewlls og VPN

1. april 2022 - Høj:Orange

Zyxel har udsendt sikkerhedsopdateringer som addresserer sårbarheder nogle af deres business firewall og VPN produkter sårbarheden har fået en CSS på 9.8!

flg produkter er ifølge Zyxel impliceret

USG/ZyWALL running firmware versions ZLD V4.20 through ZLD V4.70 (fixed in ZLD V4.71)

USG FLEX running firmware versions ZLD V4.50 through ZLD V5.20 (fixed in ZLD V5.21 Patch 1)

ATP running firmware versions ZLD V4.32 through ZLD V5.20 (fixed in ZLD V5.21 Patch 1)

VPN running firmware versions ZLD V4.30 through ZLD V5.20 (fixed in ZLD V5.21)

NSG running firmware versions V1.20 through V1.33 Patch 4 (Hotfix V1.33p4_WK11 available now, with standard patch V1.33 Patch 5 expected in May 2022)

Det anbefales at firmwareopdatere sine Zyxel-produkter

Kilde:

https://thehackernews.com/2022/03/zyxel-releases-patches-for-critical-bug.html

https://www.bleepingcomputer.com/news/security/zyxel-patches-critical-bug-affecting-firewall-and-vpn-devices/

https://www.zyxel.com/support/Zyxel-security-advisory-for-authentication-bypass-vulnerability-of-firewalls.shtml

TLSstorm sårbarhed i Avaya og Aruba

4. maj 2022 - Høj:Orange

Vi er blevet opmærksom på en kritisk sårbarhed i Avaya og Aruba switches

CVE-2022-23676 (CVSS score: 9.1) - Two memory corruption vulnerabilities in the RADIUS client implementation of Aruba switches

CVE-2022-23677 (CVSS score: 9.0) - NanoSSL misuse on multiple interfaces in Aruba switches

CVE-2022-29860 (CVSS score: 9.8) - TLS reassembly heap overflow vulnerability in Avaya switches

CVE-2022-29861 (CVSS score: 9.8) - HTTP header parsing stack overflow vulnerability in Avaya switches

HTTP POST request handling heap overflow vulnerability in a discontinued Avaya product line (no CVE)

Det anbefales af man opdaterer sine systemer

Kilder

https://www.darkreading.com/vulnerabilities-threats/tls-flaws-leave-avaya-aruba-switches-open-to-complete-takeover

https://thehackernews.com/2022/05/critical-tls-storm-20-bugs-affect-widely.html

https://www.bleepingcomputer.com/news/security/hackers-are-exploiting-critical-bug-in-zyxel-firewalls-and-vpns/

https://www.zyxel.com/support/security_advisories.shtml

https://www.rapid7.com/blog/post/2022/05/12/cve-2022-30525-fixed-zyxel-firewall-unauthenticated-remote-command-injection/

Hackere udnytter kritisk fejl i Zyxel firewalls og VPN'er

16. maj 2022 - Høj:Orange

CVE-2022-30525

CVSS 9.8

Hackere udnytter kritisk fejl i Zyxel firewalls og VPN'er

Zyxel har frigivet en patch til en kritisk sårbahed, som bliver aktivt udnyttet af cyberkriminelle.

sårbarheden tillader en ikke-autenticeret, ekstern angriber at afvikle vilkårlig kode som 'nobody' bruger på den berørte enhed.

Zyxel anbefaler at man patcher omgående!

Kilder:

Public POC på sårbarheden CVE-2022-22972 som omhandler VMware Workspace ONE, vIDM, og vRealize Automation 7.6

30. maj 2022 - Høj:Orange

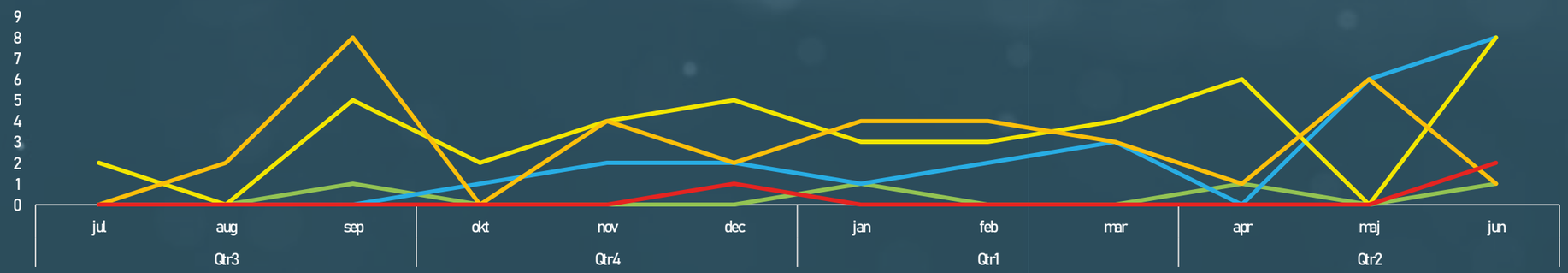
Den 19 Maj udsendte vi et varsel omkring kritiske sårbarheder I VMware.

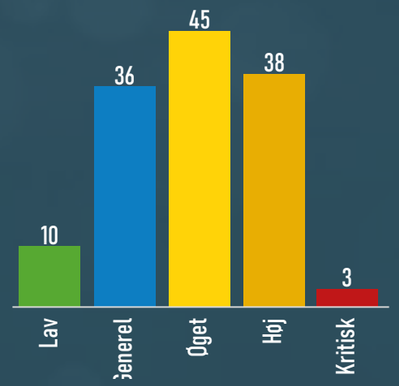
Horizon3ai har nu frigivet et Public POC på sårbarheden CVE-2022-22972 som omhandler VMware Workspace ONE, vIDM, og vRealize Automation 7.6, Der gør det muligt at omgå authentication på ovenstående produkter.

Mitigation for ovenstående er beskrevet på vmware hjemmeside:

- https://www.vmware.com/security/advisories/VMSA-2022-0014.html

Udsendte varsler de sidste 12 måneder





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