BULETINI JAVOR
16-20 TETOR 2023

Sprehja e javës

"Nëse vetëm siguria do të kishte rëndësi, kompjuterët nuk do të ndizeshin kurrë dhe të lidheshin në një rrjet me miliona ndërhyrës potencialë".

Dan Farmer

Përmbajtja:

Siguria Kibernetike në Sektorin Shëndetësor

"Sistemet në sektorin shëndetësor ishin të brishta përpara pandemisë. Pastaj sulmet e ransomware u bënë më të larmishme, më agresive dhe me kërkesa më të larta pagese."

Josh Corman

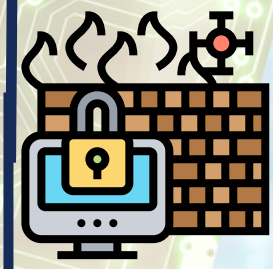
Siguria kibernetike në sektorin shëndetësor është një domosdoshmëri strategjike për çdo organizatë në industrinë mjekësore - nga ofruesit e kujdesit shëndetësor te siguruesit në kompanitë farmaceutike, bioteknologjike dhe pajisjet mjekësore.

Ai përfshin një sërë masash për të mbrojtur organizatat nga sulmet kibernetike të jashtme dhe të brendshme dhe për të siguruar disponueshmërinë e shërbimeve mjekësore, funksionimin e duhur të sistemeve dhe pajisjeve mjekësore, ruajtjen e konfidencialitetit dhe integritetit të të dhënave të pacientëve dhe pajtueshmërinë me rregulloret e industrisë.

Këshilla sigurie për sektorin shëndetësor

Parandaloni aksesin e paautorizuar

Përdorni vërtetimin me shumë faktorë i cili siguron që vetëm përdoruesit e autorizuar mund të kenë akses në të dhënat konfidenciale.



Forconi sigurinë e rrjetit

Firewall-et janë jetike për komponentët e sigurisë së rrjetit. Firewall-et bllokojnë aksesin e paautorizuar në një rrjet. Nga ana tjetër, sistemet e zbulimit të ndërhyrjeve zbulojnë dhe reagojnë ndaj kërcënimeve të mundshme kibernetike.

Kryeni përditësime të rregullta të software-it

Përditësimet e rregullta të sistemit janë masa efektive kundër vulnerabiliteteve të njohura. Ato zvogëlojnë rrezikun e sulmeve kibernetike dhe prezantojnë zgjidhjet më të fuqishme të sigurisë deri më sot.

Rruga "Papa Gjon Pali II", No.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039

BULETINI JAVOR
16-20 TETOR 2023

Shprehja e javës

"Nëse vetëm siguria do të kishte rëndësi, kompjuterët nuk do të ndizeshin kurrë dhe të lidheshin në një rrjet me miliona ndërhyrës potencialë".

Dan Farmer

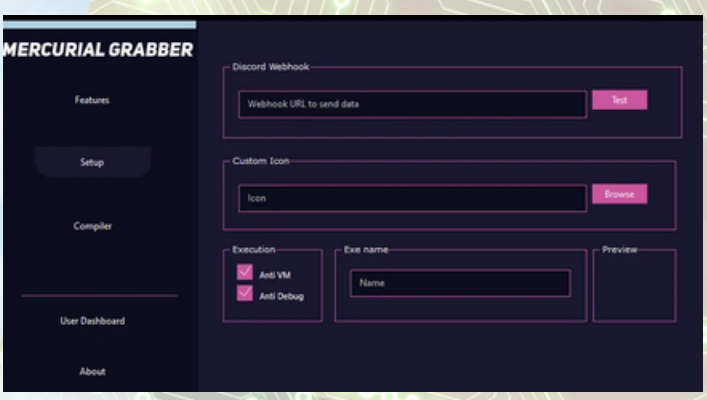
Përmbajtja:

FBI dhe CISA paralajmërojnë për sulme ransomware në sektorët kritikë të infrastrukturës

Një udhëzimi ri i përbashkët për sigurinë kibernetike i publikuar nga CISA dhe FBI si pjesë e projektit #StopRansomware shpërndan treguesit e indikatorëve, taktikave, teknikave dhe procedurave (TTP) të operacionit AvosLocker ransomware-as-a-service (RaaS) .

CISA dhe FBI rekomandojnë që organizatat të zbatojnë masat e nevojshme zbutëse për të reduktuar ndikimin e ransomware AvosLocker dhe incidente të tjera ransomware.

Link:Lexo më shumë



Platforma Discord: NJë terren mikpritës ndaj sulmeve malware

Sipas një raporti të ri nga studiuesit e Trellix, platforma Discord, një nga aplikacionet më të përdorura të komunikimit në mbarë botën, po abuzohet gjithnjë e më shumë nga sulmuesit që përdorin infrastrukturën e saj për të kryer operacionet e tyre.

Mënyra se si një sulm malware abuzon me Discord fokusohet në dy teknika kryesore: shkarkimin e skedarëve shtesë dhe nxjerrjen e informacionit.
Ndër malware-ët më të njohur të vëzhguar që kanë shënjestruar Discord janë Mercurial Grabber, Stealerium, Typhon Stealer dhe Venom RAT.

Link: Lexo më shumë

42,000 pajisje Cisco IOS XE të shfrytëzuara aktivisht

Studiuesit e sigurisë kanë gjetur mijëra hoste të shfrytëzuara lidhur me një vulnerabilitet kritik të tipit zero-day në ndërfaqen e përdoruesit në ueb të softuerit Cisco IOS XE.

Cisco njoftoi se kompania po punon për të zhvilluar një patch, megjithatë paralajmëruan se nuk ka zgjidhje ekzistuese. Kompania u bën thirrje përdoruesve të çaktivizojnë veçorinë e Serverit HTTP në sistemet e tyre.

Link: Lexo më shumë

PATCHING ALERT

Oracle - patching alert

Oracle ka publikuar 387 *patche* të reja sigurie që adresojnë 185 vulnerabilitete në kodin e tij dhe në komponentët e palëve të treta.

Më shumë se 40 patche sigurie trajtojnë vulnerabilitete të vlerësuara si kritike dhe më shumë se 200 zgjidhin dobësi që mund të shfrytëzohen remote .

AKCESK këshillon të gjithë përdoruesit e Oracle të kryejnë përditësimet e nevojshme.

Link: Lexo më shumë

Rruga "Papa Gjon Pali II", No.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039