Windows Server-en zikloaz kanpoko eguneraketa

BCSC- EGUNERAKETA-WINDOWS-SERVER

TLP:WHITE

www.basquecybersecurity.eus

2021eko azaroa

AURKIBIDEA

BCSC-ri buruz 3
1. Laburpen exekutiboa 4
2. Azterketa teknikoa 5
3. Arintzea / Konponbidea 6
4. Erreferentzia osagarriak 7

Erantzukizunetik salbuesteari buruzko klausula

Honako dokumentu hau eskaintzen da erakundeen eta interesa duten herritarren segurtasunerako, BCSCk beharrezkotzat jotzen dituen alertak ezagutzera emateko. Inongo kasutan BCSC ezin da kontsideratu hemen zabaldutako informazioaren erabilpenak zuzenean nahiz zeharka, ustekabean nahiz modu berezian, eragin litzakeen balizko kalteen arduradun. Gauza bera esan beharra dago BCSCren webean edo hortik esteken bitartez joan litekeen kanpoko web orrialdeetan, sare sozialetan, software produktuetan edo alertan nahiz BCSCren webean agertutako beste edozein informaziotan aipa litezkeen teknologiei dagokienez. Edozein kasutan, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak hemen jasotako terminoetan emandako iritzi eta gomendioak dira eta jakinarazitako informaziotik ezin da ondorioztatu ondorio juridiko loteslerik.

Salmenta debekatzeari buruzko klausula

BCSC-RI BURUZ

Zibersegurtasun Euskal Zentroa (Basque Cybersecurity Centre, BCSC) da Eusko Jaurlaritzak izendatutako entitatea Euskadin zibersegurtasunaren gaian heldutasun maila igotzeko.

BCSC erreferentziazko entitatea da zibersegurtasuna eta konfiantza digitala garatzeko Euskadiko herritar, enpresa eta instituzio publikoen artean, eta batez ere, eskualdeko ekonomiaren sektore estrategikoen kasuan.

Beraz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera dinamizatzea, eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetza proiektuak exekutatzea sustatzen du, berrikuntza teknologikoaren, ikerkuntzaren, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorretan.

Era berean, hainbat zerbitzu eskaintzen ditu Gertakarien Aurreko Ekipo modura duen rolagatik (aurrerantzean CERT, ingeleseko izenaren siglak direla-eta “Computer Emergency Response Team”). Euskal Autonomia Erkidegoko esparruan mehatxu berriak antzemateko eta horiei buruzko alerta goiztiarrak emateko gaitasuna areagotzen dihardu lanean, informazioaren segurtasun gertakarien erantzunean eta analisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:

1. LABURPEN EXEKUTIBOA

Azaroko eguneratzeak argitaratu eta astebete igaro baino lehen, Microsoft-ek zikloz kanpoko eguneratzeak egin ditu bere zerbitzari bertsioetarako.

Eguneratze horiek Windows zerbitzarietako autentifikazio arazo bat konpontzen dute, zerbitzari horiek domeinu kontrolatzaile gisa erabiltzen direnean. Konpainiaren beraren hitzetan, "*kautotzeak huts egin dezake Windows Server-en bertsio bateragarri guztietan, domeinu kontrolatzaile gisa erabiltzen denean*".

Microsoftek ere ziurtatu du akats horren ondorioz azken erabiltzaileek ezin dutela zerbitzu edo aplikazioetan saio bakarraren hasiera (Single Sign-On) erabili.

Egia da hileko ohiko programatik kanpo eguneratze bat argitaratzeko erabakia ez dela ohikoa. Hala ere, ahultasun hori konpontzeko eguneratzeak argitaratu ditu konpainiak, eta kaltetutako gailuak eguneratzeko gomendatu die erabiltzaileei. Eguneratze horiek dokumentu honetako Arintzea / Konponbidea atalean daude.

Ohiko moduan, ahultasun hori eta beste batzuk saihesteko, BCSCk gomendatzen du sistemak eta aplikazioak erabilgarri dagoen azken bertsiazken bertsioan.

2. AZTERKETA TEKNIKOA

Microsoftek salbuespen gisa argitaratu dituen eguneratze horiek, azaroko txostena argitaratu eta egun batzuetara bakarrik jakinarazi direnez, akats bat izan dute zenbait zerbitzaritan.

Microsoft-en arabera, Windows Server-ek Kerberos kautotze-tokenak nola erabiltzen zituen da arazoa. Zehazki, *S4u2self* luzapenean izandako akats baten ondorioz, Kerberosko tiketak ez ziren behar bezala kautotu. Akats horrek, lehen esan dugun bezala, baliteke autentifikazioak huts egitea domeinu kontrolatzaile gisa erabiltzen diren Windows Server sistemetan. Gainera, akats horren ondorioz, azken erabiltzaileek ezin dute zerbitzu edo aplikazioetan saio bakarraren hasiera (SSO) erabili.

Arazo horrek Windowsen bertsio hauei eragiten die:

- Windows Server 2019.
- Windows Server 2016.
- Windows Server 2012 R2.
- Windows Server 2012.
- Windows Server 2008 R2 SP1.
- Windows Server 2008 SP2.

Aurrekoarekiko mendekotasuna dela eta, enpresak jendaurrean jarri ditu ukitutako sistemetan ikusitako akatsak:

- Gertaeren bisoreak *Microsoft-Windows-Kerberos-Key-Distribution-Center* sistemaren gertaeren erregistroan erregistratutako 18 gertaera erakuts dezake.
- Errorea: 0x8009030c. Ezusteko erregistroa Azure AD aplikazioko proxy gertaeren erregistroan, 12027 ekitaldian.
- Sare-jarraipenek antzeko sinadura dute:
  - 7281 24:44 (644) 10.11.2.12.contoso.com KerberosV5 KerberosV5: TGS Request Realm: CONTOSO.COM Sname: http / xxxxx-xxx.contoso.com
  - 7282 7290 (0). CONTOSO.COM.

3. ARINTZEA / KONPONBIDEA

Microsoft-ek ahultasun horretarako zuzenketak argitaratu ditu; beraz, dagozkion eguneratzeak aplikatzea gomendatzen da:

- Windows Server 2019: KB5008602.
- Windows Server 2016: KB5008601.
- Windows Server 2012 R2: KB5008603.
- Windows Server 2012: KB5008604.
- Windows Server 2008 R2 SP1: KB5008605.
- Windows Server 2008 SP2: KB5008606.

Eguneratze horiek ezin dira Windows Update bidez aplikatu; beraz, arestian aipatutako estekak erabili behar dira, edo, bestela, Microsoft-en eguneratzeen katalogoan dagokion eguneratzea bilatu eta adierazitako jarraibideei jarraitu.

Azkenik, erroreak domeinu-kontrolatzaile gisa erabiltzen diren Windows Server sistemei bakarrik eragiten dienez, ez da beharrezkoa izango Windowsen bezero-bertsioa exekutatzen duten azken erabiltzaileen ekipoak eguneratzea.

4. ERREFERENTZIA OSAGARRIAK

- New Microsoft emergency updates fix Windows Server auth issues.
- Microsoft rolled out emergency updates to fix Windows Server auth failures.
- Actualización KB5008601.
- Actualización KB5008602.
- Actualización KB5008603.
- Actualización KB5008604.
- Actualización KB5008605.
- Actualización KB5008606.
- WSUS and the Catalog Site.
- Kerberos Authentication Overview.
- What is single sign-on in Azure Active Directory?

Gertakarien jakinarazpena

Zibersegurtasun gertakariren bat aurkitu baduzu jakinaraz iezaguzu, horrela beharrezkoak diren neurriak hartuko ditugu zabal ez dadin.

900 104 891

arazoak@bcsc.eus

Zibersegurtasun katalogoa

Zure zibersegurtasunarekin edo zure enpresarenarekin laguntza behar duzu?