Microsoften Segurtasun eguneraketak – 2021eko abendua

BCSC-EGUNERAKETA-MICROSOFT-2021-ABENDUA

TLP:WHITE

www.basquecybersecurity.eus

2021eko abendua

AURKIBIDEA

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.

Zeharkako ekimena da, Enpresa Garapenerako Euskal Agentziaren (SPRI) barnean kokatua, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren menpe dagoen sozietatea. Era berean, Eusko Jaurlaritzako beste hiru Sail ere bere parte dira: Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza; bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sistemako lau eragile ere: Tecnalia, Vicomtech, Ikerlan eta BCAM.

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, ingelesezko 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

Microsoftek 2021eko abenduko segurtasun eguneraketak argitaratu ditu. Eguneraketa honekin 67 ahultasun zuzentzen dira. Microsoftek horietatik 7 larritasun kritikotzat kalifikatu ditu eta 60 garrantzitsu modura. Horiei beste 16 ahultasun gehitu behar zaizkie, Chromium-en oinarritutako Edge nabigatzaileari partxeatu zaizkionak. Horien kasuan Redmond-eko konpainiak ez du larritasun mailarik ezarri.

Zuzendutako 67 ahultasunen artetik, 6 ahultasuni buruz aldez aurretik informazioa argitaratuta zegoen, eta horietako bat, CVE-2021-43890, aktiboki baliatua izaten ari zen.

Kaltetutako produktuen artean Microsoft Office, DirectX, Visual Studio eta Windows Media daude, beste batzuen artean.

Honako hau da ahultasunen sailkapena, euren deskripzioaren arabera:

- Ordezpen erako (spoofing) 7 ahultasun.
- Zerbitzuaren ukapen erako 3 ahultasun.
- Informazioaren hedapen erako 10 ahultasun.
- Pribilegioen eskalatze erako 21 ahultasun.
- Kodearen urruneko exekuzio erako 26 ahultasun.

Eguneraketak ahalik azkarren ezartzea gomendatzen da.

2. KALTETUTAKO BALIABIDEAK

Abenduko segurtasun partxeek honako produktu hauei eragiten dieten ahultasunekin daukate zerikusia:

- Apps
- ASP.NET Core & Visual Studio
- Azure Bot Framework SDK
- BizTalk ESB Toolkit
- Internet Storage Name Service
- Microsoft Defender for IoT
- Microsoft Devices
- Microsoft Edge (Chromium-based)
- Microsoft Local Security Authority Server (lsasrv)
- Microsoft Message Queuing
- Microsoft Office
- Microsoft Office Access
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft PowerShell
- Microsoft Windows Codecs Library
- Office Developer Platform
- Remote Desktop Client
- Role: Windows Fax Service
- Role: Windows Hyper-V
- Visual Studio Code
- Visual Studio Code - WSL Extension
- Windows Common Log File System Driver
- Windows Digital TV Tuner
- Windows DirectX
- Windows Encrypting File System (EFS)
- Windows Event Tracing
- Windows Installer
- Windows Kernel

- Windows Media
- Windows Mobile Device Management
- Windows NTFS
- Windows Print Spooler Components
- Windows Remote Access Connection Manager
- Windows Storage
- Windows Storage Spaces Controller
- Windows SymCrypt
- Windows TCP/IP
- Windows Update Stack

3. AZTERKETA TEKNIKOA

Eguneraketa hauekin zuzenduak izan diren ahultasunik garrantzitsuenak informazioa argitaratuta zeukaten 6rak dira, horietako bat aktiboki baliatua izan zena.

Baliatua izaten ari zen bakarra honakoa da:

- CVE-2021-43890: AppX-en instalatzaileak duen identitatearen ordezte erako ahultasun bat da, Windowsi eragiten diona. Microsoftek ohartarazi du badakiela CVE hau nola saiatzen ari diren baliatzen. Hain zuzen ere, Emotet, Trickbot eta Bazaloader familietako malwarea jasotzeko diseinatuta dauden paketeak sortuz ari dira baliatzen. Emaitza modura, asmo gaiztoko eragile batek, gizarte ingeniaritza bidez, biktima izango den erabiltzaile bat konbentzi lezake atxikitako fitxategia ireki dezan, horrela malwarearen infekzioa eraginez.

Informazioa argitaratuta zuten beste bostak honako hauek dira:

- CVE-2021-41333: Print spooler-en pribilegioen igotze erako ahultasuna, erasotzaile batek baliatua izateko maila baxuko baldintzak dituena. Horrek esan nahi du sarbide baldintzak ez direla oso teknikoak edo espezializatuak. Eraso bektorea modu lokaleko irakurketa/idazketa/exekuzio gaitasunetan oinarritzen da.
- CVE-2021-43240: Ahultasun honek izen laburreko pribilegioen igoera ezartzen du NTFS fitxategi sisteman. Aurrekoa bezala, baliatua izateko baldintzak baxuak dira eta bere eraso bektorea lokala da.
- CVE-2021-43880: Windows Mobile-ren gailuen administrazioak duen pribilegioen igoera erako ahultasuna, aurrekoek dituzten ezaugarri berdinekin erasoaren konplexutasunari eta eraso bektoreari dagokionez.
- CVE-2021-43883: Windows Installer-ek duen pribilegioen igoera erako ahultasuna, aurrekoek dituzten ezaugarri berdinekin erasoaren konplexutasunari eta eraso bektoreari dagokionez.
- CVE-2021-43893: Pribilegioen igotze erako ahultasuna Windowsen fitxategien zifratze sisteman (EFS). Kasu honetan eraso baten konplexutasuna altua da, eta horrek esan nahi du asmo gaiztoko eragile batek maila altuko ezagutza teknikoak izan behar dituela baliatu ahal izateko. Bestalde, eraso bektorea sare mailakoa da, eta horrek esan nahi du osagai ahula sareko pilara lotuta dagoela eta balizko erasotzaileen multzoa beste aukerek dutenetik harago doala, Internet guztia barne.

Segidan doa identifikatutako ahultasun guztien zerrenda:

CVE	Azalpena	Larritasuna	Oinarrizko CVSS	Denborazko CVSS
CVE-2021-43905	Kodearen urruneko exekuzio erako ahultasuna Microsoft Office aplikazioan	**Kritikoa**	9.6	8.6
CVE-2021-42310	Kodearen urruneko exekuzio erako ahultasuna IoTrako Microsoft Defender-en	**Kritikoa**	8.1	7.1
CVE-2021-43907	Kodearen urruneko exekuzio erako ahultasuna Visual Studio Code-ren WSL hedapenean	**Kritikoa**	9.8	8.5
CVE-2021-43899	Kodearen urruneko exekuzio erako ahultasuna Microsoften haririk gabeko 4K pantaila egokitzailean	**Kritikoa**	9.8	8.5
CVE-2021-43217	Kodearen urruneko exekuzio erako ahultasuna Windowsen fitxategien zifratze sisteman (EFS)	**Kritikoa**	8.1	7.1
CVE-2021-43233	Kodearen urruneko exekuzio erako ahultasuna Urruneko Mahaigainaren bezeroan	**Kritikoa**	7.5	6.5
CVE-2021-43215	iSNS zerbitzariarekin erlazionatuta	**Kritikoa**	9.8	8.5

	dagoen memoriako kalteen erako ahultasunak kodearen urruneko exekuzioa eragin dezake			
CVE-2021-40441	Pribilegioen igoera erako ahultasuna Windows Media Center-en	Garrantzitsua	7.8	6.8
CVE-2021-41333	Pribilegioen igotze erako ahultasuna Windowsen inprimatze ilaran	Garrantzitsua	7.8	7.2
CVE-2021-43891	Urruneko kodearen exekuzio erako ahultasuna Visual Studio Code-n	Garrantzitsua	7.8	6.8
CVE-2021-43889	Kodearen urruneko exekuzio erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	7.2	6.7
CVE-2021-43888	Informazioaren hedapen erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	7.5	7.0
CVE-2021-43882	Kodearen urruneko exekuzio erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	9.0	7.8
CVE-2021-43877	Pribilegioen igotze erako ahultasuna ASP.NET Core-n eta Visual Studio-n	Garrantzitsua	7.8	6.8
CVE-2021-43256	Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en	Garrantzitsua	7.8	6.8

CVE-2021-43255	Ordezpen erako ahultasuna Microsoft Office-n Konfiantza Zentroan	Garrantzitsua	5.5	4.8
CVE-2021-43248	Pribilegioen igotze erako ahultasuna Windows Digital Media Receiver-en	Garrantzitsua	7.8	6.8
CVE-2021-41360	Kodearen urruneko exekuzio erako ahultasuna HEVC bideo hedapenetan	Garrantzitsua	7.8	6.8
CVE-2021-41365	Kodearen urruneko exekuzio erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	8.8	7.7
CVE-2021-42294	Kodearen urruneko exekuzio erako ahultasuna Microsoft SharePoint Server-en	Garrantzitsua	7.2	6.3
CVE-2021-43247	Pribilegioen igotze erako ahultasuna Windowsen TCP/IP kontrolatzailean	Garrantzitsua	7.8	6.8
CVE-2021-42295	Informazioaren hedatze erako ahultasuna Aplikazioetarako Visual Basic-en	Garrantzitsua	5.5	4.8
CVE-2021-42309	Kodearen urruneko exekuzio erako ahultasuna Microsoft SharePoint Server-en	Garrantzitsua	8.8	7.7
CVE-2021-42320	Ordezpen erako ahultasuna Microsoft	Garrantzitsua	8.0	7.0

	Sharepoint Server-en			
CVE-2021-43207	Pribilegioen igotze erako ahultasuna Windowsen erregistro komuneko fitxategi sistemaren kontrolatzailean	Garrantzitsua	7.8	6.8
CVE-2021-43242	Ordezpen erako ahultasuna Microsoft Sharepoint Server-en	Garrantzitsua	7.6	6.6
CVE-2021-43880	Pribilegioen igoera erako ahultasuna Windows Mobile-ren gailuen administrazioan	Garrantzitsua	5.5	4.8
CVE-2021-43883	Pribilegioen igotze erako ahultasuna Windowsen Installer-en	Garrantzitsua	7.8	7.0
CVE-2021-43890	Ordezpen erako ahultasuna Windows AppX Installer-en	Garrantzitsua	7.1	6.2
CVE-2021-43892	Izenaren ordezpen erako ahultasuna Microsoft BizTalk ESB Toolkit-en	Garrantzitsua	7.4	6.7
CVE-2021-43893	Pribilegioen igotze erako ahultasuna Windowsen fitxategien zifratze sisteman (EFS)	Garrantzitsua	7.5	6.5
CVE-2021-43896	Ordezpen erako ahultasuna Microsoft PowerShell-en	Garrantzitsua	5.5	4.8

CVE-2021-43908	Identitatearen ordezpen erako ahultasuna Visual Studio Code-n	Garrantzitsua	9.6	8.6
CVE-2021-42293	Pribilegioen igotze erako ahultasuna Microsoft Jet Red-en datu baseko motorrean eta Access-en konektibitate motorrean	Garrantzitsua	6.5	5.7
CVE-2021-43246	Zerbitzuaren ukapen erako ahultasuna Windowsen Hyper-V-n	Garrantzitsua	5.6	4.9
CVE-2021-43875	Kodearen urruneko exekuzio erako ahultasuna Microsoft Office Graphics-en	Garrantzitsua	7.8	6.8
CVE-2021-43244	Informazioaren hedapen erako ahultasuna Windowsen Kernel-ean	Garrantzitsua	6.5	5.7
CVE-2021-40452	Kodearen urruneko exekuzio erako ahultasuna HEVC bideo hedapenetan	Garrantzitsua	7.8	6.8
CVE-2021-40453	Kodearen urruneko exekuzio erako ahultasuna HEVC bideo hedapenetan	Garrantzitsua	7.8	6.8
CVE-2021-42311	Kodearen urruneko exekuzio erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	8.8	7.7

CVE-2021-42312	Pribilegioen igotze erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	7.8	6.8
CVE-2021-42313	Kodearen urruneko exekuzio erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	8.8	7.7
CVE-2021-42314	Kodearen urruneko exekuzio erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	8.8	7.7
CVE-2021-42315	Kodearen urruneko exekuzio erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	8.8	7.7
CVE-2021-43245	Pribilegioen igotze erako ahultasuna Windowsen TB digitaleko sintonizadorean	Garrantzitsua	7.8	6.8
CVE-2021-43216	Informazioaren hedapen erako ahultasuna Microsoft Local Security Authority Server-en (lsasrv)	Garrantzitsua	6.5	5.7
CVE-2021-43219	Zerbitzuaren ukapen erako ahultasuna DirectX grafikoen kerneleko fitxategian	Garrantzitsua	7.4	6.4
CVE-2021-43222	Informazioaren hedapen erako ahultasuna Microsoft Message Queue Server-en	Garrantzitsua	7.5	6.5

CVE-2021-43223	Pribilegioen igoera erako ahultasuna Windowsen urruneko sarbideko konexioen Administratzailean	Garrantzitsua	7.8	6.8
CVE-2021-43224	Informazioaren hedatze erako ahultasuna Windowsen erregistro komuneko fitxategi sistemaren kontrolatzailean	Garrantzitsua	5.5	4.8
CVE-2021-43225	Kodearen urruneko exekuzio erako ahultasuna Bot Framework-en SDK-n	Garrantzitsua	7.5	6.7
CVE-2021-43226	Pribilegioen igotze erako ahultasuna Windowsen erregistro komuneko fitxategi sistemaren kontrolatzailean	Garrantzitsua	7.8	6.8
CVE-2021-43214	Kodearen urruneko exekuzio erako ahultasuna Web Media Extensions-en	Garrantzitsua	7.8	6.8
CVE-2021-43228	Zerbitzuaren ukapen erako ahultasuna SymCrypt-en	Garrantzitsua	7.5	6.5
CVE-2021-43227	Informazioaren hedapen erako ahultasuna Storage Spaces Controller-en	Garrantzitsua	5.5	4.8
CVE-2021-43243	Informazioaren hedapen erako	Garrantzitsua	5.5	4.8

	ahultasuna VP9 bideo hedapenetan			
CVE-2021-43240	Pribilegioen igotze erako ahultasuna NTFSk ezarritako izen laburrean	Garrantzitsua	7.8	7.0
CVE-2021-43239	Pribilegioen igotze erako ahultasuna Windowsen berreskuratze inguruneko Agentean	Garrantzitsua	7.1	6.2
CVE-2021-43237	Pribilegioen igotze erako ahultasuna Windowsen instalazio programan	Garrantzitsua	7.8	6.8
CVE-2021-43236	Informazioaren hedapen erako ahultasuna Microsoft Message Queue Server-en	Garrantzitsua	7.5	6.5
CVE-2021-43238	Pribilegioen igotze erako ahultasuna Windows-en urruneko sarbidean	Garrantzitsua	7.8	6.8
CVE-2021-43234	Kodearen urruneko exekuzio erako ahultasuna Windows-en fax zerbitzuan	Garrantzitsua	7.8	6.8
CVE-2021-43232	Kodearen urruneko exekuzio erako ahultasuna Windows-en gertaeren segimenduan	Garrantzitsua	7.8	6.8
CVE-2021-43231	Pribilegioen igotze erako ahultasuna Windows NTFS-n	Garrantzitsua	7.8	6.8

CVE-2021-43230	Pribilegioen igotze erako ahultasuna Windows NTFS-n	Garrantzitsua	7.8	6.8
CVE-2021-43229	Pribilegioen igotze erako ahultasuna Windows NTFS-n	Garrantzitsua	7.8	6.8
CVE-2021-43235	Informazioaren hedapen erako ahultasuna Storage Spaces Controller-en	Garrantzitsua	5.5	4.8
CVE-2021-4066	Chromium: Azpifluxu osoa ANGLE-n	Balio ezarririk gabea	9.6	8.6
CVE-2021-4061	Chromium: Moten nahasketa V8-n	Balio ezarririk gabea	9.6	8.6
CVE-2021-4065	Chromium: Askatu ondoreneko erabilpena autobetetzean	Balio ezarririk gabea	9.6	8.6
CVE-2021-4064	Chromium: Askatu ondoreneko erabilpena pantaila argazkian	Balio ezarririk gabea	9.6	8.6
CVE-2021-4063	Chromium: Erabilpena garapen tresnetan	Balio ezarririk gabea	9.6	8.6
CVE-2021-4062	Chromium: Pilako bufferraren gainezkatzea BFCache-n	Balio ezarririk gabea	9.6	8.6
CVE-2021-4059	Chromium: Datuen baliozkotze ez-nahikoa kargatzailean	Balio ezarririk gabea	9.6	8.6
CVE-2021-4052	Chromium: Erabilpena	Balio ezarririk gabea	9.6	8.6

	doakoaren ondoren web aplikazioetan			
CVE-2021-4057	Chromium: Erabilpena askapen APIaren ondoren fitxategian	Balio ezarririk gabea	9.6	8.6
CVE-2021-4056	Chromium: Motaren nahasketa kargatzailean	Balio ezarririk gabea	9.6	8.6
CVE-2021-4055	Chromium: Pilako bufferraren gainezkatzea hedapenetan	Balio ezarririk gabea	9.6	8.6
CVE-2021-4054	Chromium: Segurtasun erabiltzailearen interfaze okerra autobetetzean	Balio ezarririk gabea	9.6	8.6
CVE-2021-4053	Chromium: Erabilpena askapenaren ondoren erabiltzaile interfazean	Balio ezarririk gabea	9.6	8.6
CVE-2021-4067	Chromium: Erabilpena leihoen administratzailean	Balio ezarririk gabea	9.6	8.6
CVE-2021-4058	Chromium: Pilako bufferraren gainezkatzea ANGLE-n	Balio ezarririk gabea	9.6	8.6
CVE-2021-4068	Chromium: Konfiantzakoak ez diren sarreren baliozkotze ez-nahikoa erlaitza berriko orrialdean	Balio ezarririk gabea	9.6	8.6

4. ARINTZEA / KONPONBIDEA

Ahultasunak konpontzeko Microsoftek dagozkien segurtasun eguneraketak argitaratu ditu. Hil honetako argitalpenari buruzko oharrak eta eguneraketa gida berrikustea gomendatzen da.

5. ERREFERENTZIA OSAGARRIAK

- December 2021 Security Updates
- Security Update Guide - Microsoft
- Zero Day Initiative - The December 2021 Security Update Review

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?