Microsoften Segurtasun eguneraketa – 2022ko martxoa

BCSC-EGUNERAKETA-MICROSOFT-2022-MARTXOA

TLP:WHITE

www.basquecybersecurity.eus

2022ko martxoa

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

Zibersegurtasunaren Euskal Zentroa (Basque Cybersecurity Centre, BCSC) Eusko Jaurlaritzak zibersegurtasunaren heldutasun-maila handitzeko izendatutako erakundea da.

Zeharkako ekimena da, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren mendekoa den Enpresen Garapenerako Euskal Agentziaren (SPRI) barruan dagoena. Era berean, Eusko Jaurlaritzako beste hiru sail ere sartzen dira ekimenean –Segurtasuna, Gobernantza Publikoa eta Autogobernua eta Hezkuntza Saila–, eta Zientzia, Teknologia eta Berrikuntzaren Euskal Sareko lau eragile: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentzia-erakundea da Euskadiko herritarren, enpresen eta erakunde publikoen zibersegurtasuna eta konfiantza digitala garatzeko, bereziki eskualdeko ekonomiaren sektore estrategikoentzat.

BCSCren egitekoa da, beraz, euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa-jarduera dinamizatzea eta erreferentea izango den sektore profesional bat sortzea ahalbidetzea. Testuinguru horretan, eragile osagarrien arteko lankidetza-proiektuak gauzatzea bultzatzen da, berrikuntza teknologikoaren, ikerketaren eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren eremuetan.

Era berean, hainbat zerbitzu eskaintzen ditu Gorabeherei erantzuteko lantalde gisa (aurrerantzean CERT: “Computer Emergency Response Team” ingelesezko siglak), eta Euskal Autonomia Erkidegoaren esparruan lan egiten du mehatxu berriak detektatzeko eta garaiz ohartarazteko gaitasuna handitzen, informazioaren segurtasun-gorabeheren erantzuna eta analisia egiten, eta euskal gizartearen beharrei erantzuteko prebentzio-neurriak diseinatzen. Helburu horiek lortzeko, zibersegurtasun-gorabeherak kudeatzera bideratutako hainbat ekimenen parte da:

1. LABURPEN EXEKUTIBOA

Microsoftek 2022ko martxoko segurtasun eguneraketak argitaratu ditu. Horietan 71 ahultasun zuzentzen dituzte, 3 kritiko modura kalifikatuak eta 68 garrantzitsu gisa. Ahultasun hauek, besteak beste, honako produktuei eragiten diete: Microsoft Office, Microsoft Exchange Server, Windows Remote Desktop edo Microsoft Defender.

Ahultasunen sailkapena euren deskribapenari dagokionez honakoa da:

- Ordezpen erako (spoofing) 3 ahultasun.
- Zerbitzuaren ukapen erako 4 ahultasun.
- Informazioaren zabalkunde erako 6 ahultasun.
- Kodearen urruneko exekuzioaren erako 28 ahultasun.
- Bypass erako 3 ahultasun.
- Pribilegioen igotze erako 25 ahultasun.
- Manipulazio erako ahultasun 1 (tampering).
- Bufferraren gainezkatze erako ahultasun 1.

Ahultasun horiei Chromium-en oinarritutako Edge nabigatzailearen arazoak zuzentzen dituzten beste 21 ahultasun gehitu behar zaizkie, baina horientzat Microsoftek ez du larritasun mailarik zehaztu.

BCSCk gomendatzen du eguneraketa hauek ahalik eta azkarren aplikatzea.

2. KALTETUTAKO BALIABIDEAK

Hil honetako segurtasun partxeek honako produktu hauei eragiten dieten ahultasunekin daukate zerikusia:

- Azure Data Explorer
- . NET and Visual Studio
- Azure Site Recovery
- Endpoint-erako Microsoft Defender
- IoT-rako Microsoft Defender
- Microsoft Edge (Chromium-en oinarritua)
- Microsoft Exchange Server
- Microsoft Intune
- Microsoft Office Visio
- Microsoft Office Word
- Microsoft Windows ALPC
- Microsoft Windows Codecs Library
- Paint 3D
- Role: Windows Hyper-V
- Chrome-rako Skype Extension
- Tablet Windows User Interface
- Visual Studio Code
- WinSock-erako Windows Ancillary Function Driver
- Windows CD-ROM Driver
- Windows Cloud Files Mini Filter Driver
- Windows COM
- Windows Common Log File System Driver
- Windows DWM Core Library
- Windows Event Tracing
- Windows Fastfat Driver
- Windows Fax eta Scan Service
- Windows HTML Platform
- Windows Installer
- Windows Kernel

- Windows Media
- Windows PDEV
- Windows Point-to-Point Tunneling Protocol
- Windows Print Spooler Components
- Windows Remote Desktop
- Windows Security Support Provider Interface
- Windows SMB Server
- Windows Update Stack
- XBox

3. AZTERKETA TEKNIKOA

Eguneraketa honetan zuzendu diren ahultasun nabarmenenak 3 kritikoak dira, CVE-2022-23277, CVE-2022-24501, CVE-2022-22006, eta publikoki ezagutaraziak izan diren beste 3, CVE-2022-23285, CVE-2022-24459, CVE-2022-24512. Xehetasunak honakoak dira:

- CVE-2022-23277: Microsoft Exchange Server-i eragiten dion kodearen urruneko exekuzio erako ahultasun bat da, urrunetik balia daitekeena. Ahula den osagaiaren gaineko balizko eraso baten konplexutasuna baxua da, ez baitauka sarbiderako baldintza berezirik. Erasotzaile batek ahultasuna baliatzeko behar dituen pribilegioak oinarrizkoak dira.
- CVE-2022-24501: Aurrekoa bezala, kodearen urruneko exekuzio erako ahultasun bat da VP9 bideo luzapenen gainean, Googlek garatutako bideoen konpresiorako formatu bat. Erasoaren konplexutasuna baxua da eta ez ditu pribilegioak behar baliatua izateko.
- CVE-2022-22006: Kodearen urruneko exekuzio erako ahultasuna HEVC bideo luzapenetan. Aurrekoaren kasuan bezala, eraso bektorea lokala da. Erasoaren konplexutasuna baxua da eta asmo gaiztoko eragileak ahultasuna baliatzeko ez du inolako sarbiderik behar konfiguraziora edo fitxategietara.
- CVE-2022-21990: Kodearen urruneko exekuzio erako ahultasuna Urruneko Mahaigaineko bezeroan, publikoki ezagutarazia izan dena. Bere ezaugarriak dira sare mailako eraso bektore bat, erasoaren konplexutasun maila baxua; eta erasoa egiteko beharrezkoak diren pribilegioei dagokienez, ez da behar inolako sarbiderik konfiguraziora edo fitxategietara ahultasuna baliatzeko.
- CVE-2022-24459: Pribilegioen igotze erako ahultasuna Windowsen fax eta eskaneatze zerbitzuan, publikoki ezagutarazia. Ezaugarri modura eraso lokaleko bektore bat dauka, erasoaren konplexutasun baxua, eta erasotzaile batek ahultasuna baliatzeko behar dituen pribilegioak oinarrizkoak dira.
- CVE-2022-24512: Kodearen urruneko exekuzio erako ahultasuna .NET eta Visual Studio-n, publikoki ezagutarazia izan dena. Bere ezaugarriak dira sare mailako eraso bektore bat, erasoaren konplexutasun maila baxua; eta erasoa egiteko beharrezkoak diren pribilegioei dagokienez, ez da behar inolako sarbiderik konfiguraziora edo fitxategietara ahultasuna baliatzeko.

Honakoa da identifikatutako ahultasun guztiak zehazten dituen zerrenda:

CVE	Deskribapena	Larritasuna	Ezagutzera emana	Baliatua	CVSS
CVE-2022-23277	Kodearen urruneko exekuzio erako ahultasuna Microsoft Exchange Server-en	**Kritikoa**	Ez	Ez	8.8
CVE-2022-24501	Kodearen urruneko exekuzio erako ahultasuna VP9 bideo luzapenetan	**Kritikoa**	Ez	Ez	7.8
CVE-2022-22006	Kodearen urruneko exekuzio erako ahultasuna HEVC bideo luzapenetan	**Kritikoa**	Ez	Ez	7.8
CVE-2022-23285	Kodearen urruneko exekuzio erako ahultasuna Urruneko Mahaigaineko bezeroan	Garrantzitsua	Ez	Ez	8.8
CVE-2022-21990	Kodearen urruneko exekuzio erako ahultasuna Urruneko Mahaigaineko bezeroan	Garrantzitsua	Bai	Ez	8.8
CVE-2022-24508	Kodearen urruneko exekuzio erako ahultasuna Windows SMBv3	Garrantzitsua	Ez	Ez	8.8

	bezero/zerbitzarian				
CVE-2022-23294	Kodearen urruneko exekuzio erako ahultasuna Windowsen gertaeren segimenduan	Garrantzitsua	Ez	Ez	8.8
CVE-2022-24469	Pribilegioen igotze erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	8.1
CVE-2022-24509	Kodearen urruneko exekuzio erako ahultasuna Microsoft Office Visio-n	Garrantzitsua	Ez	Ez	7.8
CVE-2022-24452	Kodearen urruneko exekuzio erako ahultasuna HEVC bideo luzapenetan	Garrantzitsua	Ez	Ez	7.8
CVE-2022-24453	Kodearen urruneko exekuzio erako ahultasuna HEVC bideo luzapenetan	Garrantzitsua	Ez	Ez	7.8
CVE-2022-24454	Pribilegioen igotze erako ahultasuna Windowsen segurtasun zerbitzuaren hornitzailearen interfazean	Garrantzitsua	Ez	Ez	7.8
CVE-2022-24451	Kodearen urruneko exekuzio erako ahultasuna VP9	Garrantzitsua	Ez	Ez	7.8

	bideo luzapenetan				
CVE-2022-22007	Kodearen urruneko exekuzio erako ahultasuna HEVC bideo luzapenetan	Garrantzitsua	Ez	Ez	7.8
CVE-2022-24456	Kodearen urruneko exekuzio erako ahultasuna HEVC bideo luzapenetan	Garrantzitsua	Ez	Ez	7.8
CVE-2022-24457	Kodearen urruneko exekuzio erako ahultasuna HEIF irudi luzapenetan	Garrantzitsua	Ez	Ez	7.8
CVE-2022-24510	Kodearen urruneko exekuzio erako ahultasuna Microsoft Office Visio-n	Garrantzitsua	Ez	Ez	7.8
CVE-2022-24507	Windowsen funtzio laguntzailearen kontrolatzailea WinSock-ek duen pribilegioen igotze erako ahultasunerako	Garrantzitsua	Ez	Ez	7.8
CVE-2022-24455	Pribilegioen igotze erako ahultasuna Windowsen CD-ROMen kontrolatzailean	Garrantzitsua	Ez	Ez	7.8
CVE-2022-23301	Kodearen urruneko exekuzio erako ahultasuna HEVC	Garrantzitsua	Ez	Ez	7.8

	bideo luzapenetan				
CVE-2022-24461	Kodearen urruneko exekuzio erako ahultasuna Microsoft Office Visio-n	Garrantzitsua	Ez	Ez	7.8
CVE-2022-23300	Kodearen urruneko exekuzio erako ahultasuna prozesatu gabeko irudiaren luzapenean	Garrantzitsua	Ez	Ez	7.8
CVE-2022-23299	Pribilegioen igotze erako ahultasuna Windows PDEV-en	Garrantzitsua	Ez	Ez	7.8
CVE-2022-23296	Pribilegioen igotze erako ahultasuna Windows Installer-en	Garrantzitsua	Ez	Ez	7.8
CVE-2022-23295	Kodearen urruneko exekuzio erako ahultasuna prozesatu gabeko irudiaren luzapenean	Garrantzitsua	Ez	Ez	7.8
CVE-2022-23293	Pribilegioen igotze erako ahultasuna Windowsen Fast FAT fitxategi sistemaren kontrolatzailean	Garrantzitsua	Ez	Ez	7.8
CVE-2022-23291	Pribilegioen igotze erako ahultasuna Windowsen	Garrantzitsua	Ez	Ez	7.8

	DWMren liburutegi nagusian				
CVE-2022-23290	Pribilegioen igotze erako ahultasuna Windowsen eskuz idatzitako sarreraren COMean	Garrantzitsua	Ez	Ez	7.8
CVE-2022-23266	Pribilegioen igotze erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	Ez	Ez	7.8
CVE-2022-23282	Kodearen urruneko exekuzio erako ahultasuna Paint 3D-n	Garrantzitsua	Ez	Ez	7.8
CVE-2022-24459	Pribilegioen igotze erako ahultasuna Windowsen fax eta eskaneatze zerbitzuan	Garrantzitsua	Bai	Ez	7.8
CVE-2022-24464	Zerbitzuaren ukapen erako ahultasuna .NET eta Visual Studio-n	Garrantzitsua	Ez	Ez	7.5
CVE-2022-24522	Informazioaren hedapen erako ahultasuna Chrome-rako Skype-ren luzapenean	Garrantzitsua	Ez	Ez	7.5
CVE-2022-24468	Kodearen urruneko exekuzio erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	7.2

CVE-2022-24517	Kodearen urruneko exekuzio erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	7.2
CVE-2022-24470	Kodearen urruneko exekuzio erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	7.2
CVE-2022-24471	Kodearen urruneko exekuzio erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	7.2
CVE-2022-24520	Kodearen urruneko exekuzio erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	7.2
CVE-2022-23284	Pribilegioen igotze erako ahultasuna Windowsen inprimatze ilaran	Garrantzitsua	Ez	Ez	7.2
CVE-2022-24467	Kodearen urruneko exekuzio erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	7.2
CVE-2022-23265	Kodearen urruneko exekuzio erako ahultasuna IoTrako Microsoft Defender-en	Garrantzitsua	Ez	Ez	7.2
CVE-2022-24525	Pribilegioen igotze erako ahultasuna Windows Update-ren pilan	Garrantzitsua	Ez	Ez	7.0

CVE-2022-23283	Pribilegioen igotze erako ahultasuna Windows ALPC-n	Garrantzitsua	Ez	Ez	7.0
CVE-2022-21967	Pribilegioen igotze erako ahultasuna Windowserako Xbox Live-ren autentifikazio Administratzailean	Garrantzitsua	Ez	Ez	7.0
CVE-2022-23286	Pribilegioen igotze erako ahultasuna Windowsen hodeiko fitxategien mini iragazkiaren kontrolatzailean	Garrantzitsua	Ez	Ez	7.0
CVE-2022-23287	Pribilegioen igotze erako ahultasuna Windows ALPC-n	Garrantzitsua	Ez	Ez	7.0
CVE-2022-23288	Pribilegioen igotze erako ahultasuna Windowsen DWMren liburutegi nagusian	Garrantzitsua	Ez	Ez	7.0
CVE-2022-24505	Pribilegioen igotze erako ahultasuna Windows ALPC-n	Garrantzitsua	Ez	Ez	7.0
CVE-2022-23298	Pribilegioen igotze erako ahultasuna Windows NT sistema eragilearen kernelean	Garrantzitsua	Ez	Ez	7.0

CVE-2022-24460	Pribilegioen igotze erako ahultasuna Tablet Windowseko erabiltzaile interfazearen aplikazioan	Garrantzitsua	Ez	Ez	7.0
CVE-2022-23253	Zerbitzuaren ukapen erako ahultasuna puntutik punturako tunelaren protokoloan	Garrantzitsua	Ez	Ez	6.5
CVE-2022-24463	Ordezpen erako ahultasuna Microsoft Exchange Server-en	Garrantzitsua	Ez	Ez	6.5
CVE-2020-8927	Brotli-ren liburutegiaren bufferraren gainezkatze erako ahultasuna	Garrantzitsua	Ez	Ez	6.5
CVE-2022-24519	Pribilegioen igotze erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	6.5
CVE-2022-24518	Pribilegioen igotze erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	6.5
CVE-2022-24506	Pribilegioen igotze erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	6.5
CVE-2022-24515	Pribilegioen igotze erako ahultasuna Azure Site Recovery-n	Garrantzitsua	Ez	Ez	6.5

CVE-2022-24512	Kodearen urruneko exekuzio erako ahultasuna .NET eta Visual Studio-n	Garrantzitsua	Bai	Ez	6.3
CVE-2022-0807	Chromium: Inplementazio desegokia Autobete-n	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0795	Chromium: Tipoen nahasketa keinadaren diseinuan	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0796	Chromium: Doakoaren ondoreneko erabilpena hedabideetan	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0797	Chromium: Memoriarako sarbidea mugez kanpo Mojo-n	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0802	Chromium: Inplementazio desegokia pantaila osoaren moduan	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0801	Chromium: Inplementazio desegokia HTML aztertzailean	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0808	Chromium: Askapenaren ondoreneko erabilpena Chrome OS Shell-en	Balio ezarririk gabea	Ez	Ez	6.1

CVE-2022-0793	Chromium: Askapenaren ondoreneko erabilpena Views-en	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0803	Chromium: Inplementazio desegokia Baimenetan	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0800	Chromium: Pilako bufferraren gainezkatzea konbertsio erabiltzailearen interfazean	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0804	Chromium: Inplementazio desegokia pantaila osoaren moduan	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0806	Chromium: Datuen ihesa Canvas-en	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0805	Chromium: Doakoaren ondoreneko erabilpena Browser Switcher-en	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0798	Chromium: Askapenaren ondoreneko erabilpena MediaStream-en	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0799	Chromium: Zuzentarauen aplikazio ez nahikoa instalatzailean	Balio ezarririk gabea	Ez	Ez	6.1

CVE-2022-0794	Chromium: Doakoaren ondoreneko erabilpena WebShare-n	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0809	Chromium: Memoriarako sarbidea mugez kanpo WebXR-n	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0792	Chromium: Irakurketa mugetatik kanpo ANGLE-n	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0791	Chromium: Askapenaren ondoreneko erabilpena Omnibox-en	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0790	Chromium: Askapenaren ondoreneko erabilpena Cast-en erabiltzaile interfazean	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-0789	Chromium: Bufferraren gainezkatzea ANGLE-n	Balio ezarririk gabea	Ez	Ez	6.1
CVE-2022-24526	Identitatearen ordezpen erako ahultasuna Visual Studio Code-n	Garrantzitsua	Ez	Ez	6.1
CVE-2022-23278	Identitatearen ordezpen erako ahultasuna endpoint-etarako Microsoft Defender-en	Garrantzitsua	Ez	Ez	5.9

CVE-2022-21973	Zerbitzuaren ukapen erako ahultasuna Windows Media Center-en eguneraketan	Garrantzitsua	Ez	Ez	5.5
CVE-2022-23281	Informazioaren hedatze erako ahultasuna Windowsen erregistro komuneko fitxategi sistemaren kontrolatzailean	Garrantzitsua	Ez	Ez	5.5
CVE-2022-23297	Informazioaren hedapen erako ahultasuna Windows NT Lan Manager Datagram Receiver-en kontrolatzailean	Garrantzitsua	Ez	Ez	5.5
CVE-2022-24462	Windows Worden segurtasun ezaugarriaren gabezia erako ahultasuna	Garrantzitsua	Ez	Ez	5.5
CVE-2022-24511	Manipulazio erako ahultasuna Microsoft Office Worden	Garrantzitsua	Ez	Ez	5.5
CVE-2022-24503	Bezeroaren informazioaren hedapen erako ahultasuna Urruneko Mahaigainaren protokoloan	Garrantzitsua	Ez	Ez	5.4
CVE-2022-21975	Zerbitzuaren ukapen erako ahultasuna	Garrantzitsua	Ez	Ez	4.7

	Windows Hyper-V-n				
CVE-2022-22010	Informazioaren hedapen erako ahultasuna Media Foundation-en	Garrantzitsua	Ez	Ez	4.4
CVE-2022-24502	Windowsen HTML plataformen segurtasun ezaugarriaren gabezia erako ahultasuna	Garrantzitsua	Ez	Ez	4.3
CVE-2022-24465	Segurtasun ezaugarriaren gabezia erako ahultasuna Mac-erako Microsoft Intune-ren Atarian	Garrantzitsua	Ez	Ez	3.3
CVE-2022-21977	Informazioaren hedapen erako ahultasuna Media Foundation-en	Garrantzitsua	Ez	Ez	3.3

4. ARINTZEA / KONPONBIDEA

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

5. ERREFERENTZIA GEHIGARRIAK

- March 2022 Security Updates
- Security Update Guide - Microsoft
- Zero Day initiative-The March 2022 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?