Microsoft-en Segurtasun buletina 2020ko azaroa

BCSC_AHULTASUNA_BULETINA_SEGURTASUN_MICROSOFT_AZAROA_2020

TLP:WHITE

2020ko azaroa

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 inplikatzen ditu: 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:

LABURPEN EXEKUTIBOA

Microsoftek 2020ko azaroko segurtasun partxeei buruzko bere hileroko buletina argitaratu du, “Patch Tuesday” izenez ezaguna.

Hil honetako buletinean konpainiak 112 segurtasun akats zuzendu ditu, bere hainbat produktutan daudenak: Microsoft Windows, Office, Internet Explorer (IE), Edge, Exchange Server, Azure Sphere, Windows Defender, Microsoft Teams, Visual Studio eta abar.

Horietatik 17 ahultasun kritikoak dira, 93 garrantzitsuak eta 2 kritikotasun baxukoak. Horiek guztien artetik bakarra izaten ari da asmo gaiztoz baliatua, eta horregatik akats horiek konpontzeko segurtasun partxeak ahalik azkarren aplikatzea gomendatzen da.

AZTERKETA TEKNIKOA

Konfirmatu ahal izan denez, argitaratu diren 112 ahultasunen artetik bat besterik ez da izaten ari aktiboki baliatua.

Microsoftek emandako informazioaren arabera, ahultasunari CVE-2020-17087 identifikatzailea esleitu zaio eta Windows 7 eta Windows 10eko erabiltzaileen gainean izan da baliatua.

Erabiltzaileak Chromek duen ahultasun bat baliatzen ari dira (CVE-2020-15999, 86.0.4240.111 bertsioan partxeatua) Chromen asmo gaiztoko kodea exekutatzeko eta, ondoren, Windowsen Zero Day-ren bidez, Chromeren segurtasun sandbox-a saihesteko eta kodearen gainean pribilegioak igotzeko, Sistema Eragilea erasotu ahal izatearren.

Ahultasun honetarako Microsoften Buletinaren informazioaren arabera, Zero Day-a Windowsen Kernelean kokatzen da, eta gaur egun Windowsen zerbitzudun bertsio guztiei eragiten die. Horrek barne hartzen ditu Windows 7ren ondorengo bertsio guztiak eta Windows Server-en hedapen guztiak.

Aurkitutako gainerako ahultasunak honakoak dira:

Ahultasun Kritikoak:

- CVE-2020-17105: Urruneko kodearen exekuzioa AV1 bideo hedapenaren gainean.
- CVE-2020-16988: Pribilegioen Igoera erako ahultasuna Azure Sphere-n.
- CVE-2020-17048: Chakra-n memoriaren hondatzearen scripting erako ahultasuna.
- CVE-2020-17101: Urruneko kodearen exekuzio erako ahultasuna HEIF irudi hedapenetan.
- CVE-2020-17106: Urruneko kodearen exekuzio erako ahultasuna HEVC irudi hedapenetan.
- CVE-2020-17107: Urruneko kodearen exekuzio erako ahultasuna HEVC irudi hedapenetan.
- CVE-2020-17108: Urruneko kodearen exekuzio erako ahultasuna HEVC irudi hedapenetan.
- CVE-2020-17109: Urruneko kodearen exekuzio erako ahultasuna HEVC irudi hedapenetan.
- CVE-2020-17110: Urruneko kodearen exekuzio erako ahultasuna HEVC irudi hedapenetan.
- CVE-2020-17053: Memoriaren hondatze erako ahultasuna Internet Explorer-en.

- CVE-2020-17058: Memoriaren hondatze erako ahultasuna Microsoft-en arakatzailean.
- CVE-2020-17078: Kodearen urruneko exekuzioaren erako ahultasuna Raw Image-n.
- CVE-2020-17079: Kodearen urruneko exekuzioaren erako ahultasuna Raw Image-n.
- CVE-2020-17082: Kodearen urruneko exekuzioaren erako ahultasuna Raw Image-n.
- CVE-2020-17052: Scripting motorrean memoriaren hondatze erako ahultasuna.
- CVE-2020-17051: Urruneko kodearen exekuzio erako ahultasuna Windows Network File System-en.
- CVE-2020-17042: Urruneko kodearen exekuzio erako ahultasuna Windows Print Spooler-en.

Ahultasun Garrantzitsuak:

- CVE-2020-1325: Spoofing erako ahultasuna Azure DevOps Server eta Team Foundation Services-en.
- CVE-2020-16986: Zerbitzuaren ukazio erako ahultasuna Azure Sphere-n.
- CVE-2020-16981: Pribilegioen Igoera erako ahultasuna Azure Sphere-n.
- CVE-2020-16989: Pribilegioen Igoera erako ahultasuna Azure Sphere-n.
- CVE-2020-16992: Pribilegioen Igoera erako ahultasuna Azure Sphere-n.
- CVE-2020-16993: Pribilegioen Igoera erako ahultasuna Azure Sphere-n.
- CVE-2020-16985: Informazioaren ezagutarazte erako ahultasuna Azure Sphere-n.
- CVE-2020-16990: Informazioaren ezagutarazte erako ahultasuna Azure Sphere-n.
- CVE-2020-16983: Manipulazio erako ahultasuna Azure Sphere-n.
- CVE-2020-16970: Sinatu gabeko kodearen exekuzio erako ahultasuna Azure Sphere-n.
- CVE-2020-16982: Sinatu gabeko kodearen exekuzio erako ahultasuna Azure Sphere-n.
- CVE-2020-16984: Sinatu gabeko kodearen exekuzio erako ahultasuna Azure Sphere-n.
- CVE-2020-16987: Sinatu gabeko kodearen exekuzio erako ahultasuna Azure Sphere-n.

- CVE-2020-16991: Sinatu gabeko kodearen exekuzio erako ahultasuna Azure Sphere-n.
- CVE-2020-16994: Sinatu gabeko kodearen exekuzio erako ahultasuna Azure Sphere-n.
- CVE-2020-17054: Chakra-n memoriaren hondatzearen scripting erako ahultasuna.
- CVE-2020-16998: Pribilegioen igoera DirectX-n.
- CVE-2020-17049: Bypass erako ahultasuna Kerberos Security Feature-n.
- CVE-2020-17090: Endpoint Security Feature-rako Microsoft Defender-en bypass-a.
- CVE-2020-17005: Cross-site Scripting erako ahultasuna Microsoft Dynamics 365-en.
- CVE-2020-17006: Cross-site Scripting erako ahultasuna Microsoft Dynamics 365-en.
- CVE-2020-17018: Cross-site Scripting erako ahultasuna Microsoft Dynamics 365-en.
- CVE-2020-17021: Cross-site Scripting erako ahultasuna Microsoft Dynamics 365-en.
- CVE-2020-17019: Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en.
- CVE-2020-17064: Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en.
- CVE-2020-17065: Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en.
- CVE-2020-17066: Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en.
- CVE-2020-17067: Microsoft Excel Security Feature-ren bypass-a.
- CVE-2020-17085: Zerbitzuaren ukapen erako ahultasuna Microsoft Exchange-ren zerbitzarietan.
- CVE-2020-17083: Urruneko kodearen exekuzio erako ahultasuna Microsoft Exchange-ren zerbitzarietan.
- CVE-2020-17084: Urruneko kodearen exekuzio erako ahultasuna Microsoft Exchange-ren zerbitzarietan.
- CVE-2020-17062: Urruneko kodearen exekuzio erako ahultasuna Microsoft Office Access Connectivity Engine-n.
- CVE-2020-17063: Spoofing erako ahultasuna Microsoft Office Onlinen.

- CVE-2020-17081: Informazioaren agerpen erako ahultasuna Microsoft Raw Image hedapenean.
- CVE-2020-17086: Informazioaren agerpen erako ahultasuna Microsoft Raw Image hedapenean.
- CVE-2020-16979: Informazioaren agerpen erako ahultasuna Microsoft Sharepoint hedapenean.
- CVE-2020-17017: Informazioaren agerpen erako ahultasuna Microsoft Sharepoint hedapenean.
- CVE-2020-17061: Urruneko kodearen exekuzio erako ahultasuna Microsoft Sharepoint-en.
- CVE-2020-17016: Spoofing erako ahultasuna Microsoft Sharepoint-en.
- CVE-2020-17060: Spoofing erako ahultasuna Microsoft Sharepoint-en.
- CVE-2020-17091: Urruneko kodearen exekuzio erako ahultasuna Microsoft Teams-en.
- CVE-2020-17020: Bypass erako ahultasuna Microsoft Word Security Feature-n.
- CVE-2020-17000: Informazioaren agerpen erako ahultasuna RDPren (Remote Desktop Protocol) Bezeroan.
- CVE-2020-16997: Informazioaren agerpen erako ahultasuna RDPren (Remote Desktop Protocol) Zerbitzarian.
- CVE-2020-17104: Urruneko kodearen exekuzio erako ahultasuna Visual Studio Code JSHint-en hedapenean.
- CVE-2020-17100: Manipulazio erako ahultasuna Vulnerabilidad Studio-n.
- CVE-2020-17102: Informazioaren agerpen erako ahultasuna WebP Image hedapenetan.
- CVE-2020-17010: Pribilegioen igoera erako ahultasuna Win32k-en.
- CVE-2020-17038: Pribilegioen igoera erako ahultasuna Win32k-en.
- CVE-2020-17013: Informazioaren agerpen erako ahultasuna Win32k-en.
- CVE-2020-17012: Pribilegioen igoera erako ahultasuna Windows Bind Filter-en.
- CVE-2020-17113: Informazioaren agerpen erako ahultasuna Windows Camera Codec-en.
- CVE-2020-17029: Informazioaren agerpen erako ahultasuna Windows Canonical Display Driver-en.
- CVE-2020-17024: Pribilegioen igoera erako ahultasuna Windows Client Side Rendering Print-en.

- CVE-2020-17088: Pribilegioen igoera erako ahultasuna Windows Common Log File System Driver-en.
- CVE-2020-17071: Informazioaren agerpen erako ahultasuna Windows Delivery Optimization-en.
- CVE-2020-17007: Informazioaren agerpen erako ahultasuna Windows Error Reporting-en.
- CVE-2020-17036: Informazioaren agerpen erako ahultasuna Windows Function Discovery-n.
- CVE-2020-17068: Urruneko kodearen exekuzio erako ahultasuna Windows GDI+-en.
- CVE-2020-17004: Informazioaren agerpen erako ahultasuna Windows Graphics Component-en.
- CVE-2020-17040: Segurtasun funtzioen bypass erako ahultasuna Windows Hyper-V-n.
- CVE-2020-17035: Pribilegioen igoera erako ahultasuna Windows kernel-en.
- CVE-2020-17045: Informazioaren agerpen erako ahultasuna Windows KernelStream-en.
- CVE-2020-17030: Informazioaren agerpen erako ahultasuna Windows MSCTF Server-en.
- CVE-2020-17069: Informazioaren agerpen erako ahultasuna Windows NDIS-en.
- CVE-2020-17047: Zerbitzuaren ukapen erako ahultasuna Windows Network File System-en.
- CVE-2020-17056: Informazioaren agerpen erako ahultasuna Windows Network File System-en.
- CVE-2020-17011: Pribilegioen igoera erako ahultasuna Windows Port Class Library-n.
- CVE-2020-17041: Pribilegioen igoera erako ahultasuna Windows Print Configuration-en.
- CVE-2020-17001: Pribilegioen igoera erako ahultasuna Windows Print Spooler-en.
- CVE-2020-17014: Pribilegioen igoera erako ahultasuna Windows Print Spooler-en.
- CVE-2020-17025: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.
- CVE-2020-17026: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.

- CVE-2020-17027: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.
- CVE-2020-17028: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.
- CVE-2020-17031: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.
- CVE-2020-17032: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.
- CVE-2020-17033: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.
- CVE-2020-17034: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.
- CVE-2020-17043: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.
- CVE-2020-17044: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.
- CVE-2020-17055: Pribilegioen igoera erako ahultasuna Windows Remote Access-en.
- CVE-2020-1599: Spoofing erako ahultasuna Windowsen.
- CVE-2020-17070: Pribilegioen igoera erako ahultasuna Windows Update Medic Service-n.
- CVE-2020-17073: Pribilegioen igoera erako ahultasuna Windows Update Orchestrator Service-n.
- CVE-2020-17074: Pribilegioen igoera erako ahultasuna Windows Update Orchestrator Service-n.
- CVE-2020-17076: Pribilegioen igoera erako ahultasuna Windows Update Orchestrator Service-n.
- CVE-2020-17077: Pribilegioen igoera erako ahultasuna Windows Update Stack-en.
- CVE-2020-17075: Pribilegioen igoera erako ahultasuna Windows USO Core Worker-en.
- CVE-2020-17037: Pribilegioen igoera erako ahultasuna Windows WalletService-n.
- CVE-2020-16999: Informazioaren agerpen erako ahultasuna Windows WalletService-n.
- CVE-2020-17057: Pribilegioen igoera erako ahultasuna Windows Win32k-en.

Kritikotasun baxuko ahultasunak:

- CVE-2020-17015: Spoofing erako ahultasuna Microsoft Sharepoint-en.
- CVE-2020-17046: Informazioaren agerpen erako ahultasuna Windows Error Reporting-en.

Kaltetutako baliabideak

2020ko azaroko segurtasun partxeak ondorengo produktuei eragiten dieten segurtasun ahultasunekin daukate zerikusia:

- Azure Devops
- Azure Sphere
- Microsoft Windows Codecs Library
- Visual Studio
- Microsoft Teams
- Windows Defender
- Common Log File System Driver
- Windows Kernel
- Microsoft Exchange Server
- Windows Update Stack
- Windows NDIS
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Browsers
- Microsoft Windows
- Microsoft Scripting Engine
- Windows WalletService
- Microsoft Dynamics

ARINTZEA / KONPONBIDEA

Patch Tuesday-en jasotako ahultasun guztiak arintzeko eta partxeatzeko, Microsoftek dagozkien segurtasun eguneraketak argitaratzen ditu, eta horiekin batera beren release note-ak ere bai, guztiak Security Update Guide-n erabilgarri.

ERREFERENTZIA OSAGARRIAK

- Microsoft Security Update Guide
- CVE-2020-17087 Detail
- CVE-2020-15999 Detail

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?