Microsoften Segurtasun Eguneraketa – 2021eko azaroa

BCSC-EGUNERAKETA-MICROSOFT-2021-AZAROA

TLP:WHITE

www.basquecybersecurity.eus

2021eko 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 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, 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

Microsoftek 2021eko azaroko segurtasun eguneraketei buruzko bere hileroko buletina argitaratu du, “Patch Tuesday” izenez ezaguna. Eguneraketa honekin 55 ahultasun zuzentzen dira. Microsoftek horietatik 6 larritasun kritikotzat kalifikatu ditu eta 49 garrantzitsu modura.

Zuzendutako 55 ahultasun horien artetik lau ezagutzen ziren aldez aurretik (CVE-2021-38631, CVE-2021-41371, CVE-2021-43208, CVE-2021-43209) eta bi baliatuak izaten ari ziren erasotzaileen aldetik (CVE-2021-42292 eta CVE-2021-42321).

Kaltetutako produktuen artean, besteak beste, honakoak daude: Azure, Microsoft Excel, Microsoft Access, Microsoft Sharepoint, Microsoft Active Directory, Visual Studio eta Edge nabigatzailea.

Honako hau da ahultasunen sailkapena, euren deskripzioaren arabera:

- Pribilegioen eskalatze erako 20 ahultasun.
- Ordezpen erako (spoofing) 4 ahultasun.
- Zerbitzuaren ukapen erako 3 ahultasun.
- Kodearen urruneko exekuzio erako 13 ahultasun.
- Informazioaren hedapen erako 10 ahultasun.
- Segurtasun ezaugarriei buruzko bypass erako 2 ahultasun.
- Bufferraren gainezkatze erako ahultasun 1.
- Memoriaren hondatze erako ahultasun 1.
- Manipulazio erako ahultasun 1 Azure Sphere-n.

Kaltetutako produktuen eguneraketak ahalik azkarren ezartzea gomendatzen da.

2. KALTETUTAKO BALIABIDEAK

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

- 3D Viewer
- Azure
- Azure RTOS
- Azure Sphere
- Microsoft Dynamics
- Microsoft Edge (Chromium-based)
- Microsoft Edge (Chromium-based) in IE Mode
- Microsoft Exchange Server
- Microsoft Office
- Microsoft Office Access
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft Windows
- Microsoft Windows Codecs Library
- Power BI
- Role: Windows Hyper-V
- Visual Studio
- Visual Studio Code
- Windows Active Directory
- Windows COM
- Windows Core Shell
- Windows Cred SSProvider Protocol
- Windows Defender
- Windows Desktop Bridge
- Windows Diagnostic Hub
- Windows Fastfat Driver
- Windows Feedback Hub
- Windows Hello

- Windows Installer
- Windows Kernel
- Windows NTFS
- Windows RDP
- Windows Scripting
- Windows Virtual Machine Bus

3. AZTERKETA TEKNIKOA

Eguneraketa hauekin zuzendutako ahultasun nabarmenenak dira aurrez ezagunak ziren lau ahultasunak eta erasotzaileak baliatzen ari ziren biak:

Gaur egun baliatuak izaten ari diren biak honakoak dira:

- CVE-2021-42321: Segurtasun eguneraketak Exchange-ri eragiten dion kodearen urruneko exekuzio erako akats bat zuzentzen du, publikoki ezagutarazia izan ez dena. Hori garrantzitsua da urte honen hasieran Microsoft Exchange zerbitzariak exekutatzen zituzten erakunde gehienei 0 day erako lau erasok eragin zietelako, erasotzaileei backdoor-ak instalatzea eta posta elektronikoa desbideratzea ahalbidetzen zietenak.
- CVE-2021-42292: Eguneraketa honek Microsoft Exceli eragiten dio, 2013tik 2021era bitarteko bertsioetan. Kaltetutako Excel bertsio bat erasotzeko bereziki diseinatua izan den fitxategi bat irekitzean kodea urrunetik exekutatzea ahalbidetzen duen akats bat zuzentzen du. Oraindik ez dago argi makro bat den edo kalkulu orrietan kodea kargatzeko beste moduren bat den. Aipatu beharra dago Mac-eko Officen erabiltzaileentzat eguneraketa ez dagoela oraindik eskuragarri buletin hau argitaratzeko datan, eta ez duela jakinarazpen publikorik izan.

Gainerako laurak publikoki ezagutaraziak izan dira eta honako hauek dira:

- CVE-2021-38631: Protokoloaren informazioaren hedapen erako ahultasuna (RDP), Windows 7 eta 11n eta Windows Server 2008-2019n presente dagoen urruneko administrazioko tresna. Erasotzaile batek segurtasun zuloa baliatuz gero, Windowseko RDP bezeroen pasahitzak eskura litzake RDP zerbitzariaren administratzaileen aldetik.
- CVE-2021-41371: Protokoloaren informazioaren hedapen erako ahultasuna (RDP), aurreko CVEaren ezaugarri eta baliatze modu berdinak dituena.
- CVE-2021-43208: 3D Viewer-i eragin dio, Microsoften errealitate areagotuko aplikazioa denari. Diotenez segurtasun zulo hau baliatzea ez da oso litekeena.
- CVE-2021-43209: Honek ere 3d Viewer errealitate areagotuko aplikazioari eragiten dio, eta aurreko CVEaren modu berdinean. Microsoftek dio nekez gerta daitekeela hori baliatzea.

Segidan doa identifikatutako ahultasun guztien zerrenda:

CVE	Azalpena	Larritasuna
CVE-2021-3711	OpenSSL: SM2ren deszifratze bufferraren gainezkatzea CVE-2021-3711	**Kritikoa**
CVE-2021-42298	Kodearen urruneko exekuzio erako ahultasuna Microsoft Defender-en	**Kritikoa**
CVE-2021-42316	Kodearen urruneko exekuzio erako ahultasuna Microsoft Dynamics 365-en (lokala)	**Kritikoa**
CVE-2021-26443	Kodearen urruneko exekuzio erako ahultasuna Microsoft Virtual Machine Bus-en (VMBus)	**Kritikoa**
CVE-2021-42279	Memoriaren hondatze erako ahultasuna Chakra-ren scripting motorrean	**Kritikoa**
CVE-2021-38666	Kodearen urruneko exekuzio erako ahultasuna Urruneko Mahaigainaren bezeroan	**Kritikoa**
CVE-2021-36957	Pribilegioen eskalatze erako ahultasuna Windows Desktop Bridge-n	Garrantzitsua
CVE-2021-40442	Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen	Garrantzitsua
CVE-2021-41351	Microsoft Edge-ren ordezpena (Chromen oinarritua) IE moduan	Garrantzitsua
CVE-2021-41356	Zerbitzuaren ukapen erako ahultasuna Windowsen	Garrantzitsua
CVE-2021-41370	Pribilegioen igotze erako ahultasuna NTFS-n	Garrantzitsua
CVE-2021-41373	Informazioaren hedapen erako ahultasuna FSLogix-en	Garrantzitsua
CVE-2021-41374	Informazioaren hedapen erako ahultasuna Azure Sphere-n	Garrantzitsua

CVE-2021-41375	Informazioaren hedapen erako ahultasuna Azure Sphere-n	Garrantzitsua
CVE-2021-41376	Informazioaren hedapen erako ahultasuna Azure Sphere-n	Garrantzitsua
CVE-2021-42277	Pribilegioen igotze erako ahultasuna Diagnostikoen kontzentratzailearen biltzaile estandarrean	Garrantzitsua
CVE-2021-42283	Pribilegioen igotze erako ahultasuna NTFS-n	Garrantzitsua
CVE-2021-42284	Zerbitzuaren ukapen erako ahultasuna Windowsen Hyper-V-n	Garrantzitsua
CVE-2021-42285	Pribilegioen igotze erako ahultasuna Windowsen kernelean	Garrantzitsua
CVE-2021-42286	Windows Core Shell SI Host Extension Framework pribilegioen igotze erako ahultasunerako Shell konposagarrian	Garrantzitsua
CVE-2021-42287	Pribilegioen igotze erako ahultasuna Active Directory-ren Domeinu zerbitzuetan	Garrantzitsua
CVE-2021-42288	Windows Hello-ren segurtasun ezaugarriaren gabezia erako ahultasuna	Garrantzitsua
CVE-2021-42291	Pribilegioen igotze erako ahultasuna Active Directory-ren Domeinu zerbitzuetan	Garrantzitsua
CVE-2021-42292	Windows Excelen segurtasun ezaugarriaren gabezia erako ahultasuna	Garrantzitsua
CVE-2021-42296	Kodearen urruneko exekuzio erako ahultasuna Microsoft Worden	Garrantzitsua
CVE-2021-42305	Microsoft Exchange Server-en ordezpen erako ahultasuna	Garrantzitsua
CVE-2021-42321	Kodearen urruneko exekuzio erako ahultasuna Microsoft Exchange Server-en	Garrantzitsua

CVE-2021-42282	Pribilegioen igotze erako ahultasuna Active Directory-ren Domeinu zerbitzuetan	Garrantzitsua
CVE-2021-38665	Bezeroaren informazioaren hedapen erako ahultasuna Urruneko Mahaigainaren protokoloan	Garrantzitsua
CVE-2021-43208	Kodearen urruneko exekuzio erako ahultasuna 3D Viewer-en	Garrantzitsua
CVE-2021-42323	Informazioaren hedapen erako ahultasuna Azure RTOS-en	Garrantzitsua
CVE-2021-38631	Informazioaren hedapen erako ahultasuna Windowsen Urruneko mahaigainaren protokoloan (RDP)	Garrantzitsua
CVE-2021-41349	Microsoft Exchange Server-en ordezpen erako ahultasuna	Garrantzitsua
CVE-2021-41366	Pribilegioen igotze erako ahultasuna Kredentzialen segurtasunarekiko bateragarritasunaren hornitzaile protokoloan (CredSSP)	Garrantzitsua
CVE-2021-41367	Pribilegioen igotze erako ahultasuna NTFS-n	Garrantzitsua
CVE-2021-41368	Kodearen urruneko exekuzio erako ahultasuna Microsoft Access-en	Garrantzitsua
CVE-2021-41371	Informazioaren hedapen erako ahultasuna Windowsen Urruneko mahaigainaren protokoloan (RDP)	Garrantzitsua
CVE-2021-41372	Power BIren txostenen zerbitzariaren ordezpen erako ahultasuna	Garrantzitsua
CVE-2021-41377	Pribilegioen igotze erako ahultasuna Windowsen Fast FAT fitxategi sistemaren kontrolatzailean	Garrantzitsua
CVE-2021-41378	Kodearen urruneko exekuzio erako ahultasuna Windows NTFS-n	Garrantzitsua

CVE-2021-41379	Pribilegioen igotze erako ahultasuna Windowsen Installer-en	Garrantzitsua
CVE-2021-43209	Kodearen urruneko exekuzio erako ahultasuna 3D Viewer-en	Garrantzitsua
CVE-2021-42274	Zerbitzuaren ukapen erako ahultasuna Windows Hyper-V-ren gailu diskretuen (DDA) esleipenean	Garrantzitsua
CVE-2021-42276	Kodearen urruneko exekuzio erako ahultasuna Microsoft Windows Media Foundation-en	Garrantzitsua
CVE-2021-42278	Pribilegioen igotze erako ahultasuna Active Directory-ren Domeinu zerbitzuetan	Garrantzitsua
CVE-2021-42280	Pribilegioen igotze erako ahultasuna Windowsen Iruzkinen zentroan	Garrantzitsua
CVE-2021-42300	Manipulazio erako ahultasuna Azure Sphere-n	Garrantzitsua
CVE-2021-42301	Informazioaren hedapen erako ahultasuna Azure RTOS-en	Garrantzitsua
CVE-2021-42302	Pribilegioen igotze erako ahultasuna Azure RTOS-en	Garrantzitsua
CVE-2021-42303	Pribilegioen igotze erako ahultasuna Azure RTOS-en	Garrantzitsua
CVE-2021-42304	Pribilegioen igotze erako ahultasuna Azure RTOS-en	Garrantzitsua
CVE-2021-42319	Pribilegioen igotze erako ahultasuna Visual Studio-n	Garrantzitsua
CVE-2021-42322	Pribilegioen igotze erako ahultasuna Visual Studio Code-n	Garrantzitsua
CVE-2021-42275	Kodearen urruneko exekuzio erako ahultasuna Windowserako Microsoft COM-en	Garrantzitsua
CVE-2021-26444	Informazioaren hedapen erako ahultasuna Azure RTOS-en	Garrantzitsua

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

- November 2021 Security Updates
- Security Update Guide - Microsoft
- Zero Day Initiative - The November 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?