Microsoften Segurtasun Eguneraketa - 2020ko Abendua

BCSC-EGUNERAKETA-MICROSOFT-2020-ABENDUA

TLP:WHITE

www.basquecybersecurity.eus

2020ko 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

Guztiz debekatuta dago dokumentu hau saltzea edo beragatik edozein onura ekonomiko eskuratzea, baina posible da bera kopiatzea, banatzea, hedatzea edo ezagutzera ematea.

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

Hil honetan 58 ahultasunetarako zuzenketak argitaratu dira, ondoko produktu hauei eragiten dietenak: Microsoft Exchange, Hyper-V, Windows NTFS, suite Office-ren aplikazioak (Excel, Power Point, SharePoint, Outlook), Edge nabigatzailea eta abar.

Horietatik 9 ahultasun kritikoak dira, 47 garrantzitsuak eta 2 kritikotasun ertainekoak. Horien guztien artean ez dago inolako zero-day-rik ezta aldez aurretik baliatua izan den ahultasunik ere.

2. AZTERKETA TEKNIKOA

Ez da antzeman aktiboki baliatua izaten ari den ahultasunik. Nolanahi ere, argitaratutako ahultasunetako batzuk bereziki garrantzitsuak dira, baliatuak izanez gero izango luketen eraginarengatik:

- **CVE-2020-17095 - Hyper-V** - Urruneko kodearen exekuzio erako ahultasuna: Hyper-V Makina Birtual batean asmo gaiztoko programak ahalbidetzen ditu eta, ondorioz, Host-ean kodea exekuta daiteke.
- **CVE-2020-17096 - Windows NTFS** – Urruneko kodearen exekuzio erako ahultasuna: ahultasun hau lokalki balia daiteke pribilegioak igotzeko, eta baita urrunetik ere, SMBv2-ren bidez, komandoak exekutatzeko.
- **CVE-2020-17099 - Windows Lock Screen** – Bypass-a segurtasun neurrietan: erasotzaile lokal batek komandoak exekuta ditzake blokeatuta dagoen Windows gailu batetik.

Ahultasunak konpontzeko partxeez gain, Microsoftek SAD DNS izenaz ezagutzen den DNS cachearen pozoitze erako ahultasunari buruzko ohartarazpena argitaratu du, duela gutxi Tsinghua eta Kaliforniako ikertzaileek aurkitua. Ohartarazpenak workaround bat ere jasotzen du ahultasun hori Windowseko erregistroa aldatuz konpontzeko edo arintzeko, UDP paketeen gehieneko tamaina 1221 bytetara aldatuta. Balio hori baino handiagoko eskaeren kasuan, DNS resolver-a TCP konexioetara aldatuko da.

Ondoren doa identifikatutako ahultasun guztiak zehazten dituen zerrenda:

Ahultasun Kritikoak:

- CVE-2020-17158 Urruneko kodearen exekuzio erako ahultasuna Microsoft Dynamics 365 for Finance and Operations-en
- CVE-2020-17152 Urruneko kodearen exekuzio erako ahultasuna Microsoft Dynamics 365 for Finance and Operations-en
- CVE-2020-17131 Memoriaren hondatze erako ahultasuna Chakra Scripting Engine-n.
- CVE-2020-17117 Urruneko kodearen exekuzio erako ahultasuna Microsoft Exchange-n.
- CVE-2020-17132 Urruneko kodearen exekuzio erako ahultasuna Microsoft Exchange-n.
- CVE-2020-17142 Urruneko kodearen exekuzio erako ahultasuna Microsoft Exchange-n.
- CVE-2020-17121 Urruneko kodearen exekuzio erako ahultasuna Microsoft SharePoint-en.
- CVE-2020-17118 Urruneko kodearen exekuzio erako ahultasuna Microsoft SharePoint-en.

- CVE-2020-17095 Urruneko kodearen exekuzio erako ahultasuna Hyper-V-n.

Ahultasun Garrantzitsuak:

- CVE-2020-17145 Spoofing erako ahultasuna Azure DevOps Server and Team Foundation Services-en.
- CVE-2020-17135 Spoofing erako ahultasuna Azure DevOps Server-en.
- CVE-2020-17002 Bypass-a Azure SDK for C-ren segurtasun neurrietan.
- CVE-2020-16971 Bypass-a Azure SDK for Java Security-ren segurtasun neurrietan.
- CVE-2020-17160 Bypass-a Azure Sphere Security-ren segurtasun neurrietan (Ezeztua).
- CVE-2020-17147 Cross-site scripting erako ahultasuna Dynamics CRM Webclient-en.
- CVE-2020-17133 Informazioaren Agerpen erako ahultasuna Microsoft Dynamics Business Central/NAV-en.
- CVE-2020-17143 Informazioaren agerpen erako ahultasuna Microsoft Exchange-n.
- CVE-2020-17144 Urruneko kodearen exekuzio erako ahultasuna Microsoft Exchange-n.
- CVE-2020-17141 Urruneko kodearen exekuzio erako ahultasuna Microsoft Exchange-n.
- CVE-2020-17137 Pribilegioak igotze erako ahultasuna DirectX Graphics-en.
- CVE-2020-17098 Informazioaren agerpen erako ahultasuna Windows GDI+en.
- CVE-2020-17130 Bypass erako ahultasuna Microsoft Excel-en segurtasun neurrietan.
- CVE-2020-17128 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en.
- CVE-2020-17129 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en.
- CVE-2020-17124 Urruneko kodearen exekuzio erako ahultasuna Microsoft PowerPoint-en.
- CVE-2020-17123 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en.
- CVE-2020-17119 Urruneko kodearen exekuzio erako ahultasuna Microsoft Outlook-en.

- CVE-2020-17125 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en.
- CVE-2020-17127 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en.
- CVE-2020-17126 Informazioaren agerpen erako ahultasuna Microsoft Excel-en.
- CVE-2020-17122 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excel-en.
- CVE-2020-17120 Informazioaren agerpen erako ahultasuna Microsoft SharePoint-en.
- CVE-2020-17089 Pribilegioen igotze erako ahultasuna Microsoft SharePoint-en.
- CVE-2020-17136 Pribilegioen igotze erako ahultasuna Windows Cloud Files Mini Filter Driver-en.
- CVE-2020-16996 Bypass erako ahultasuna Kerberos-en segurtasun neurrietan.
- CVE-2020-17138 Informazioaren agerpen erako ahultasuna Windows Error Reporting-en.
- CVE-2020-17092 Pribilegioen igotze erako ahultasuna Windows Network Connections Service-n.
- CVE-2020-17139 Bypass erako ahultasuna Windows Overlay Filter-en segurtasun neurrietan.
- CVE-2020-17103 Pribilegioen igotze erako ahultasuna Windows Cloud Files Mini Filter Driver-en.
- CVE-2020-17134 Pribilegioen igotze erako ahultasuna Windows Cloud Files Mini Filter Driver-en.
- CVE-2020-17148 Urruneko kodearen exekuzio erako ahultasuna Visual Studio Code Remote Development Extension-en.
- CVE-2020-17159 Urruneko kodearen exekuzio erako ahultasuna Visual Studio Code Java Extension Pack-en.
- CVE-2020-17156 Urruneko kodearen exekuzio erako ahultasuna Visual Studio-n.
- CVE-2020-17150 Urruneko kodearen exekuzio erako ahultasuna Visual Studio-n.
- CVE-2020-16960 Urruneko kodearen exekuzio erako ahultasuna Windows Backup Engine-n.
- CVE-2020-16958 Urruneko kodearen exekuzio erako ahultasuna Windows Backup Engine-n.

- CVE-2020-16959 Urruneko kodearen exekuzio erako ahultasuna Windows Backup Engine-n.
- CVE-2020-16961 Urruneko kodearen exekuzio erako ahultasuna Windows Backup Engine-n.
- CVE-2020-16964 Urruneko kodearen exekuzio erako ahultasuna Windows Backup Engine-n.
- CVE-2020-16963 Urruneko kodearen exekuzio erako ahultasuna Windows Backup Engine-n.
- CVE-2020-16962 Pribilegioen igotze erako ahultasuna Windows Backup Engine-n.
- CVE-2020-17094 Informazioaren agerpen erako ahultasuna Windows Error Reporting-en.
- CVE-2020-17099 Bypass erako ahultasuna Windows Lock Screen-en segurtasun neurrietan.
- CVE-2020-17097 Pribilegioen igotze erako ahultasuna Windows Digital Media Receiver-en.
- CVE-2020-17096 Urruneko kodearen exekuzio erako ahultasuna Windows NTFS-en.
- CVE-2020-17140 Informazioaren agerpen erako ahultasuna Windows SMB-n.

Larritasun ertaineko ahultasunak:

- CVE-2020-17153 Spoofing erako ahultasuna Android-erako Microsoft Edge-n.
- CVE-2020-17115 Spoofing erako ahultasuna Microsoft Sharepoint-en.

2.1 Kaltetutako baliabideak

2020ko abenduko segurtasun partxeek honako produktu hauei eragiten dieten segurtasun ahultasunekin daukate zerikusia:

- Azure Devops
- Azure SDK
- Azure Sphere
- Microsoft Dynamics
- Microsoft Edge
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Windows
- Microsoft Windows DNS
- Visual Studio
- Windows Backup Engine
- Windows Error Reporting
- Windows Hyper-V
- Windows Lock Screen
- Windows Media
- Windows SMB

3. ARINTZEA / KONPONBIDEA

2020ko abenduko 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.

4. ERREFERENTZIA OSAGARRIAK

- Microsoft Security Update Guide
- December 2020 Security Updates
- Segurtasun eguneraketaren inplementazioari buruzko informazioa: asteartea, 2020ko abenduaren 8a
- Microsoft Guidance for Addressing Spoofing Vulnerability in DNS Resolver

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?