Microsoften Segurtasun Eguneraketa - 2021eko Urtarrila

BCSC-EGUNERAKETA-MICROSOFT-2021-URTARRILA

TLP:WHITE

www.basquecybersecurity.eus

2021eko urtarrila

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

Hil honetan 83 ahultasunetarako zuzenketak argitaratu dira, ondoko produktu hauei eragiten dietenak: Microsoft Defender, Visual Studio, Hyper-V, WalletService, Office suitearen aplikazioak (Excel, Power Point, SharePoint, Outlook), Edge nabigatzailea eta abar.

Horietatik 10 ahultasun kritikoak dira eta 73 garrantzitsu modura sailkatu dira. Horien guztien artetik Microsoft Defender-i eragiten dion Zero Day erako ahultasun baten berri eman da, eta itxura denez dagoeneko baliatua izan da. Era berean, Windows splwow64 zerbitzuan joan den abenduan ezagutzera emandako beste ahultasun bat ere argitaratu da, Microsoften informazioen arabera orain arte baliatua izan ez dena.

Horiek denak konpondu egiten dira argitalpenari lotutako segurtasun partxea aplikatuz.

2. AZTERKETA TEKNIKOA

2021eko urtarrileko Patch Tuesday honetan Microsoftek ezagutzera emandako ahultasunen artetik Zero Day erako bat antzeman da, eta uste da bere berri eman aurretik eta bere konponbidea argitaratu aurretik baliatua izan dela.

Ahultasunak **CVE-2021-1647** kodea dauka, eta hori baliatuz urruneko kodea exekuta daiteke Microsoft Defender-en segurtasun softwarean. Microsoft Malware Protection Engine-ren 1.1.17600.5 bertsioa bitartean dauka eragina. Konponbidea 1.1.17700.4 bertsioan eta geroagokoetan aplikatu da eta horiek dagoeneko ez dira bertsio ahulak.

Microsoftek erabiltzaileei eta sistemen administratzaileei eskatzen die eguneraketen azken bertsioa deskargatuta eta instalatuta daukatela egiaztatzea. Microsoft Malware Protection Enginek aldioro eta automatikoki egiten dituen eguneraketak dira, erabiltzaileak inolako ekintzarik egin behar izan gabe. Nolanahi ere, eskuz ere eragin daiteke eguneraketa.

Bestalde, buletinean beste ahultasun bat ere jasotzen da, 2020ko abenduaren 15ean Trend Micro`s Zero Day Initiativek ezagutzera eman zuena eta, Microsoften arabera, baliatua izan ez dena. Ahultasun honek **CVE-2021-1648** kodea dauka eta baliatua izan daiteke pribilegioak igotzeko Windows splwow64 zerbitzuko eraso baten aurrean.

Ondoren doa identifikatutako ahultasun guztiak zehazten dituen zerrenda:

Ahultasun Kritikoak:

- CVE-2021-1668 Urruneko kodearen exekuzio erako ahultasuna Microsoft DTV-DVD Video Decoder-en
- CVE-2021-1705 Memoriaren hondatze erako ahultasuna Microsoft Edge-n (HTML-based)
- CVE-2021-1665 Urruneko kodearen exekuzio erako ahultasuna GDI+-en
- CVE-2021-1647 Kodearen urruneko exekuzio erako ahultasuna Microsoft Defender-en
- CVE-2021-1643 Urruneko kodearen exekuzio erako ahultasuna HEVC Video Extensions-en
- CVE-2021-1666 Urruneko kodearen exekuzio erako ahultasuna Remote Procedure Call Runtime-n
- CVE-2021-1673 Urruneko kodearen exekuzio erako ahultasuna Remote Procedure Call Runtime-n
- CVE-2021-1658 Urruneko kodearen exekuzio erako ahultasuna Remote Procedure Call Runtime-n
- CVE-2021-1667 Urruneko kodearen exekuzio erako ahultasuna Remote Procedure Call Runtime-n

- CVE-2021-1660 Urruneko kodearen exekuzio erako ahultasuna Remote Procedure Call Runtime-n

Ahultasun Garrantzitsuak:

- CVE-2021-1725 Informazioaren agerpen erako ahultasuna Bot Framework SDK-n
- CVE-2021-1723 Zerbitzuaren ukapen erako ahultasuna ASP.NET Core eta Visual Studio-n
- CVE-2021-1677 Spoofing erako ahultasuna Azure Active Directory Pod Identity-n
- CVE-2021-1683 Bypass erako ahultasuna Windows Bluetooth-en segurtasun neurrietan
- CVE-2021-1638 Bypass erako ahultasuna Windows Bluetooth-en segurtasun neurrietan
- CVE-2021-1684 Bypass erako ahultasuna Windows Bluetooth-en segurtasun neurrietan
- CVE-2021-1709 Pribilegioen igoera erako ahultasuna Windows Win32k-n
- CVE-2021-1696 Informazioaren agerpen erako ahultasuna Windows Graphics Component-en
- CVE-2021-1708 Informazioaren agerpen erako ahultasuna Windows GDI+-en
- CVE-2021-1713 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen
- CVE-2021-1714 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen
- CVE-2021-1711 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen
- CVE-2021-1715 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen
- CVE-2021-1716 Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen
- CVE-2021-1712 Pribilegioen igotze erako ahultasuna Microsoft SharePointen
- CVE-2021-1707 Urruneko kodearen exekuzio erako ahultasuna Microsoft SharePoint Server-en
- CVE-2021-1718 Manipulazio erako ahultasuna Microsoft SharePoint Server-en
- CVE-2021-1717 Spoofing erako ahultasuna Microsoft SharePointen

- CVE-2021-1719 Pribilegioen igotze erako ahultasuna Microsoft SharePointen
- CVE-2021-1641 Spoofing erako ahultasuna Microsoft SharePointen
- CVE-2021-1702 Pribilegioen igotze erako ahultasuna Windows Remote Procedure Call Runtime-n
- CVE-2021-1649 Pribilegioen igotze erako ahultasuna Active Template Library-n.
- CVE-2021-1676 Informazioaren agerpen erako ahultasuna Windows Nt Lan Manager Datagram Receiver Driver-en
- CVE-2021-1689 Pribilegioen igoera erako ahultasuna Windows Multipoint Management-en
- CVE-2021-1657 Urruneko kodearen exekuzio erako ahultasuna Windows Fax Compose Form-en
- CVE-2021-1646 Pribilegioen igoera erako ahultasuna Windows WLAN Service-n
- CVE-2021-1650 Pribilegioen igotze erako ahultasuna Windows Runtime C++ Template Library-n
- CVE-2021-1706 Pribilegioen igoera erako ahultasuna Windows Luafv-en
- CVE-2021-1699 Informazioaren agerpen erako ahultasuna Windowsen (modem.sys)
- CVE-2021-1644 Urruneko kodearen exekuzio erako ahultasuna HEVC Video Extensions-en
- CVE-2021-1637 Informazioaren agerpen erako ahultasuna Windows DNS Query-n
- CVE-2021-1636 Pribilegioen igotze erako ahultasuna Microsoft SQL-n
- CVE-2020-26870 Urruneko kodearen exekuzio erako ahultasuna Visual Studio-n
- CVE-2021-1642 Pribilegioen igoera erako ahultasuna Windows AppX Deployment Extensions-en
- CVE-2021-1685 Pribilegioen igoera erako ahultasuna Windows AppX Deployment Extensions-en
- CVE-2021-1679 Zerbitzuaren ukapen erako ahultasuna Windows CryptoAPI-n
- CVE-2021-1652 Pribilegioen igoera erako ahultasuna Windows CSC Service-n
- CVE-2021-1654 Pribilegioen igoera erako ahultasuna Windows CSC Service-n

- CVE-2021-1659 Pribilegioen igoera erako ahultasuna Windows CSC Service-n
- CVE-2021-1653 Pribilegioen igoera erako ahultasuna Windows CSC Service-n
- CVE-2021-1655 Pribilegioen igoera erako ahultasuna Windows CSC Service-n
- CVE-2021-1693 Pribilegioen igoera erako ahultasuna Windows CSC Service-n
- CVE-2021-1688 Pribilegioen igoera erako ahultasuna Windows CSC Service-n
- CVE-2021-1680 Pribilegioen igoera erako ahultasuna Diagnostics Hub Standard Collector-en
- CVE-2021-1651 Pribilegioen igoera erako ahultasuna Diagnostics Hub Standard Collector-en
- CVE-2021-1645 Informazioaren agerpen erako ahultasuna Windows Docker-en
- CVE-2021-1703 Pribilegioen igoera erako ahultasuna Windows Event Logging Service-n
- CVE-2021-1662 Pribilegioen igoera erako ahultasuna Windows Event Tracing-en
- CVE-2021-1691 Zerbitzuaren ukapen erako ahultasuna Hyper-V-en
- CVE-2021-1704 Pribilegioen igoera erako ahultasuna Hyper-V-n.
- CVE-2021-1692 Zerbitzuaren ukapen erako ahultasuna Hyper-V-en
- CVE-2021-1661 Pribilegioen igoera erako ahultasuna Windows Installer-en
- CVE-2021-1697 Pribilegioen igoera erako ahultasuna Windows InstallService-n
- CVE-2021-1682 Pribilegioen igoera erako ahultasuna Windows Kernel-en
- CVE-2021-1710 Kodearen urruneko exekuzio erako ahultasuna Microsoft Windows Media Foundation-en
- CVE-2021-1678 Bypass erako ahultasuna NTLMren segurtasun neurrietan
- CVE-2021-1695 Pribilegioen igoera erako ahultasuna Windows Print Spooler-en
- CVE-2021-1663 Informazioaren agerpen erako ahultasuna Windows Projected File System FS Filter Driver-en

- CVE-2021-1672 Informazioaren agerpen erako ahultasuna Windows Projected File System FS Filter Driver-en
- CVE-2021-1670 Informazioaren agerpen erako ahultasuna Windows Projected File System FS Filter Driver-en
- CVE-2021-1674 Bypass erako ahultasuna Windows Remote Desktop Protocol Core-ren segurtasun neurrietan
- CVE-2021-1669 Bypass erako ahultasuna Windows Remote Desktop-en segurtasun neurrietan
- CVE-2021-1701 Urruneko kodearen exekuzio erako ahultasuna Remote Procedure Call Runtime-n
- CVE-2021-1700 Urruneko kodearen exekuzio erako ahultasuna Remote Procedure Call Runtime-n
- CVE-2021-1664 Urruneko kodearen exekuzio erako ahultasuna Remote Procedure Call Runtime-n
- CVE-2021-1671 Urruneko kodearen exekuzio erako ahultasuna Remote Procedure Call Runtime-n
- CVE-2021-1648 Pribilegioen igotze erako ahultasuna Microsoft splwow64-en
- CVE-2021-1656 Informazioaren agerpen erako ahultasuna TPM Device Driver-en
- CVE-2021-1694 Pribilegioen igoera erako ahultasuna Windows Update Stack-en
- CVE-2021-1686 Pribilegioen igoera erako ahultasuna Windows WalletService-n
- CVE-2021-1681 Pribilegioen igoera erako ahultasuna Windows WalletService-n
- CVE-2021-1690 Pribilegioen igoera erako ahultasuna Windows WalletService-n
- CVE-2021-1687 Pribilegioen igoera erako ahultasuna Windows WalletService-n

2.1 Kaltetutako baliabideak

2021eko urtarrileko segurtasun partxeek honako produktu hauei eragiten dieten segurtasun ahultasunekin daukate zerikusia:

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft Windows Codecs Library
- Visual Studio
- SQL Server
- Microsoft Malware Protection Engine
- .NET Core
- .NET Repository
- ASP .NET
- Azure

3. ARINTZEA / KONPONBIDEA

2021eko urtarrileko 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
- January 2021 Security Updates
- Microsoft patches Defender antivirus zero-day exploited in the wild
- Microsoft January 2021 Patch Tuesday fixes 83 flaws, 1 zero-day

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?