SAPen segurtasun eguneraketak – 2022ko otsaila

BCSC-EGUNERAKETAK-SAP-2022-OTSAILA

TLP:WHITE

www.basquecybersecurity.eus

2022ko otsaila

EDUKIAREN TAULA

Erantzukizunetik salbuesteko klausula

Dokumentu hau ematen da BCSCk erakundeen eta herritar interesdunen segurtasunaren alde beharrezkotzat jotzen dituen alertak zabaltzeko. BCSC ezin da inola ere jo zuzenean edo zeharka, ustekabean edo ohiz kanpo, jakinarazitako informazioa erabiltzeak eragin ditzakeen kalteen erantzuletzat, ez eta BCSCren webgunetik nahiz kanpoko informaziotik (kanpoko web-orrialdeetarako, sare sozialetarako, software-produktuetarako edo BCSCren edo webgunearen bidez ager daitekeen beste edozein informaziotarako esteken bidez) aipatzen diren teknologien erantzuletzat ere. Nolanahi ere, alertaren edukiak eta mezu elektronikoen bidez eman daitezkeen erantzunak hemen jasotako terminoen araberako iritziak eta gomendioak dira, eta ezingo da ondorio juridiko loteslerik sortu jakinarazitako informaziotik.

Saltzeko debekuaren 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

Hilero bezala, 2022ko otsailaren 8an, SAPek produktu askorentzako segurtasun eguneraketak argitaratu ditu. Hilabete honetan, 19 segurtasun ohar argitaratu dira guztira, eta horietako 9 kritikoak dira.

Bereziki garrantzitsuak dira SAP ingurunea bateratzen duen eta enpresei negozio eta datu prozesuak integratzeko aukera ematen dien SAP NetWeaver plataformari eragiten dioten guztiak. Log4j kalteberatasunari zuzenketak egiten jarraitzen da (SAP Commerce, SAP Data Intelligence eta SAP Customer Checkout tresnei eragiten die). Azkenik, zuzenketak egin zaizkio Google Chromium nabigatzaileari SAP Bussiness Client tresnaren gain.

BCSCk eguneraketak aplikatzea gomendatzen du, sistemak seguru mantentzeko.

2. KALTETUTAKO BALIABIDEAK

Hilabete honetako segurtasun eguneraketak produktu hauei eragiten dieten kalteberatasunei lotuta daude:

- SAP Web Dispatcher - 7.49, 7.53, 7.77, 7.81, 7.85, 7.22 EXT, 7.86, 7.87 bertsioak
- SAP Content Server - 7.53 bertsioak
- SAP NetWeaver eta ABAP Platform - KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49 bertsioak
- SAP Commerce - 1905, 2005, 2105, 2011 bertsioak
- SAP Data Intelligence - 3. bertsioa
- Internet of Things Edge Platform - 4.0 bertsioa
- SAP Customer Checkout - 2. bertsioa
- SAP Business Client - 6.5 bertsioa
- SAP Solution Manager (diagnostikoaren erroko kausaren analisi-tresnak) - 720 bertsioa
- SAP S/4HANA - 100, 101, 102, 103, 104, 105, 106 bertsioak
- SAP NetWeaver Application Server Java - KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53 bertsioak
- SAP NetWeaver AS ABAP (Workplace Server) - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787 bertsioak
- SAP NetWeaver (ABAP and Java application Servers) - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756 bertsioak
- SAP ERP HCM (Portugal) - 600, 604, 608 bertsioak
- SAP Business Objects Web Intelligence (BI Launchpad) - 420 bertsioa
- SAP 3D Visual Enterprise Viewer - 9.0 bertsioa
- SAP Adaptive Server Enterprise - 16.0 bertsioa
- SAP S/4HANA (hornitzaileen informazio-orria eta bazkide komertzialen, hornitzaileen eta bezeroen enpresa-bilaketa) - 104, 105, 106 bertsioak
- SAP NetWeaver Application Server for ABAP (Kernel) eta ABAP Platform (Kernel) - KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49 bertsioak

3. ANALISI TEKNIKOA

Behean, argitaratutako segurtasun-oharrei buruzko informazioa eskaintzen da:

Segurtasun-oharra	Lehentasuna	CVSS
3123396 CVE-2022-22536 :Eskaeren kontrabandoa eta eskaeren kateatzea (SAP NetWeaver, SAP Content Server eta SAP Web Dispatcher)	**Kritikoa**	10
3142773 CVE-2021-44228 :Apache Log4j 2 osagaiarekin lotutako kodearen urruneko exekuzioaren kalteberatasuna (SAP Commerce) Lotutako CVEak: CVE-2021-45046, CVE-2021-45105, CVE-2021-44832	**Kritikoa**	10
3130920 Apache Log4j 2 osagaiarekin lotutako kodearen urruneko exekuzioaren kalteberatasuna (SAP Data Intelligence 3) (lokala) Lotutako CVEak: CVE-2021-44228, CVE-2021-45046, CVE-2021-45105	**Kritikoa**	10
3139893 Apache Log4j 2 osagaiarekin lotutako kodearen urruneko exekuzioaren kalteberatasuna (SAP Dynamic Authorization Management) Lotutako CVEak: CVE-2021-44228, CVE-2021-45046	**Kritikoa**	10
3132922 2021eko abenduan argitaratutako segurtasun-oharraren eguneratzea: [CVE-2021-44228] Apache Log4j 2 osagaiarekin lotutako kodearen urruneko exekuzioaren kalteberatasuna (IoT plataforma perimetrala). Lotutako CVEak: CVE-2021-45105, CVE-2021-45046 , CVE-2021-44832	**Kritikoa**	10
3133772 2021eko abenduan argitaratutako segurtasun-oharraren eguneratzea: [CVE-2021-44228] Apache Log4j 2 osagaiarekin lotutako kodearen urruneko exekuzioaren	**Kritikoa**	10

kalteberatasuna (SAP Customer Checkout) Lotutako CVEak: CVE-2021-45046, CVE-2021-45105		
3131047 2021eko abenduan argitaratutako segurtasun-oharraren eguneratzea: [CVE-2021-44228] Segurtasun-oharra Apache Log4j 2 osagaiarekin lotutako kalteberatasunaren kodearen urruneko exekuziorako	**Kritikoa**	10
2622660 2018ko apirileko adabakiaren egunean argitaratutako segurtasun-oharraren eguneratzea: SAP Business Client-ekin entregatutako Google Chromium nabigatzailearen kontrolerako segurtasun-eguneratzeak	**Kritikoa**	10
3140940 [CVE-2022-22544] Funtzioen bereizketa falta da (SAP Solution Manager). Diagnostikoaren erroko kausaren analisi-tresnak	**Kritikoa**	9.1
3112928 2022ko urtarrileko adabakiaren egunean argitaratutako segurtasun-oharraren eguneratzea: [CVE-2022-22531] Kalteberatasun ugari (F0743) Ordainketa bakarreko aplikazioa sortzea (SAP S/4HANA) CVE gehigarria- CVE-2022-22530	Altua	8.7
3123427 [CVE-2022-22532] HTTP eskaeren kontrabandoa (SAP NetWeaver Server Java aplikazioa)	Altua	8.1
3140587 [CVE-2022-22540] SQL injekzioaren kalteberatasuna (SAP NetWeaver AS ABAP) (Workplace Server)	Altua	7.1
3124994 [CVE-2022-22534] Guneen arteko komando-sekuentzien kalteberatasuna (XSS) (SAP NetWeaver)	Ertaina	4.7
3126489 [CVE-2022-22535] Baimen-egiaztapena falta da (SAP ERP HCM)	Ertaina	6.5

3126748 [CVE-2022-22546] XSS kalteberatasuna (SAP Business Objects Web Intelligence) (BI Launchpad)	Ertaina	5.4
3134684 [CVE anitzak] Sarrera okerraren balidazioa (SAP 3D Visual Enterprise Viewer) Lotutako CVEak: CVE-2022-22537, CVE-2022-22539, CVE-2022-22538	Ertaina	4.3
3140564 [CVE-2022-22528] Informazio-hedapena (SAP Adaptive Server Enterprise)	Ertaina	5.6
3142092 [CVE-2022-22542] Informazio-hedapenaren kalteberatasuna (SAP S/4HANA) (hornitzailearen informazio-orria eta bazkide komertzialen, hornitzaileen eta bezeroen enpresa-bilaketa)	Ertaina	6.5
3116223 [CVE-2022-22543] Zerbitzu-ukatzea (DOS) (SAP NetWeaver Application Server ABAP (Kernel) eta ABAP Platform-erako (Kernel))	Txikia	3.7

4. ARINTZEA / KONPONBIDEA

SAPek hilero argitaratutako segurtasun-oharrei buruzko informazioa argitaratzen du bere web-orrian.

5. ERREFERENTZIA GEHIGARRIAK

- SAP Security Patch Day – February 2022

Gorabeheraren berri ematea

Zibersegurtasun-gorabeheraren bat detektatu baduzu, jakinaraz iezaguzu neurri egokiak har ditzagun ez hedatzeko.

900 104 891

incidencias@bcsc.eus

Zibersegurtasun-katalogoa

Laguntza behar duzu zure zibersegurtasunarekin edo zure enpresarenarekin?