Ahultasunak PcVue SCADA/HMIn

BCSC_ALERTA_Ahultasunak_PcVue_SCADA/HMI

TLP:WHITE

www.basquecybersecurity.eus

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

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 eta Azpiegitura 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

Segurtasun-ikertzaileek PcVue SCADA/HMI konponbidean larriak izan daitezkeen zenbait ahultasun argitaratu dituzte. Izan ere, monitorizazio eta kontrol industrialeko softwarea da, eta, horri esker, autentifikatu gabeko urruneko erasotzaile batek kodea exekutatu, informazio konfidentziala eskuratu eta zerbitzua eten dezake.

Ikerketak **hiru ahultasun** identifikatu ditu. Horietako batek **larria** kalifikazioa jaso du, interfazean jasotako mezuak modu ez-seguruan deserializatzearekin lotuta baitago, **eta kode urruneko exekuzioa** ekar lezake. Beste bi ahultasunak larritasun handikotzat jo dira, horietako bat **DoS erasoak** egiteko aprobetxa zitekeelako; bestea, berriz, informazioa zabaltzeko arazoa da, erasotzaile **bati erabiltzaile legitimoen saio-datuak** atzitzeko aukera emango liokeena. Erreportajeen arabera, akats horien ustiapena nahiko erraza da, eta ez du erabiltzaile baten interakziorik behar.

PcVue, ARC Informatique, garatu eta mantentzeaz arduratzen den enpresa frantsesak dagoeneko konpondu ditu ahultasun horiek, produktuaren **12.0.17** bertsioa merkaturatuta, eta arintze-neurriak hartu ditu, gerta daitezkeen erasoak saihesteko. Gainera, Estatu Batuetako Azpiegitura eta Zibersegurtasunaren Segurtasun Agentziak (CISA) ere ohar bat argitaratu du, erakundeei akats horiek sortzen dituzten arriskuen berri emateko.

AZTERKETA TEKNIKOA

Zenbait ahultasun argitaratu dira **PcVue** softwareari dagokionez. Ingurune industrialak kontrolatzera bideratuta dago, eta **Microsoften** erabiltzaile-interfazearen azken funtzioak eta **Windows** plataformen segurtasun-funtzioak ditu. Produktuak fidagarritasun eta errendimendu estandar industrialak betetzen ditu, eta erabiltzaile bakar baten aplikazioak administratzeko gai da, hala nola bezero-zerbitzari aplikazioak edo HTML5 Web motako bezero arinen aplikazioak, eta arkitektura erredundante birtualizatuak eta erabilgarritasun handikoak ezartzeko aukera ematen du.

Hona hemen atzemandako hiru ahultasunen xehetasun teknikoak:

- **CVE-2020-26867**: PcVuek 12.0.17 baino lehenagoko bertsioetan, konfiantzazkoak ez diren datuen deserializazioak eragindako ahultasuna du, ez baitu behar bezala egiaztatzen lortutako datuak baliozkoak direnik. Horren ondorioz, **erasotzaile batek urrunetik egin ditzake kodeak** web-ean eta *back-end* zerbitzari mugikorrean.

  Ahultasunak **9.8ko** scorea jaso du, **CVSSv3.1** eskalaren arabera; hau da, akats kritikoa da, urrunetik ustiatu baitaiteke, konplexutasun txikikoa eta erabiltzaile batek pribilegioak edo interakzioa eskatu gabe.

- **CVE-2020-26868**: PcVue, 12.0.17 baino lehenagoko bertsioetan, **zerbitzua ukatzeko (DoS)** eraso baten aurrean zaurgarria da, baimenik gabeko erabiltzaile batek aukera baitu web-bezero legitimoek bidalitako mezuak baliozkotzeko erabilitako informazioa aldatzeko. *Web Services Toolkit-en* oinarritutako hirugarrenen sistemei ere eragiten die arazoak.

  Erasotzaile batek aldagai bat aldatzea lortzen badu ustekabeko balioak izan ditzan, aldaketak eragingo lituzke kodearen beste zati batzuen suposizioetan. Gainera, aldagai pribatu bat irakurtzekotan, informazio konfidentziala eman edo eraso gehiago egitea erraztu dezake.

- **CVE-2020-26869**: PcVue, 12.0.17 baino lehenagoko bertsioetan, **baimenik gabeko informazio-erakusketa** baten aurrean zaurgarria da, eta, horri esker, baimenik ez duten erabiltzaileek bidezko erabiltzaileen saio-datuak eskuratu ahal izango dituzte. Aurreko ahultasunak bezala, arazo horrek *Web Services Toolkit-en* oinarritutako hirugarrenen sistemei ere eragiten die.

Azken bi ahultasunek **7.5**eko score bat jaso dute **CVSSv3.1** eskalaren arabera, hau da, larritasun handiko akatsak dira, urrunetik ustiagarriak baitira, konplexutasun txikikoak eta erabiltzaile baten pribilegioak edo elkarreragina behar ez dutenak.

Orain arte, ez da sareko ustiapen aktiboei buruzko txostenik ezagutzen, ez eta hiru ahultasun horietarako exploit-ak edo kontzeptu-probak eskura dauden ere.

Ahultasun bakoitzaren deskribapenean aipatu den bezala, **PcVu-**eren bertsioak **8.10**etik **12.0.17**ra bitartekoak dira, sartu gabe.

ARINTZEA / KONPONBIDEA

ARC Informatiquek dagoeneko merkaturatu du **PcVue**-ren **12.0.17** bertsioa, eta akats horiek konpondu ahal izateko, eguneratze hori aplikatu behar da, eta PcVue-ren laguntza-zerbitzuarekin harremanetan jarri, softwarearen azken bertsioa deskargatu eta instalatzeko jarraibideak jasotzeko.

Tartean aipatutako eguneratzea alde batera utzita, fabrikatzaileak arintze-neurri hauek ezartzea gomendatzen du, erasoak izateko arriskua murrizteko:

- *Backend web* eta mugikorra duten osagaiak erabiltzen ez dituzten edo behar ez dituzten erabiltzaileen terminaletan desinstalatzea.
- 12.0.* baino lehenagoko bertsioetan *backend web* eta mugikorraren konfigurazio lehenetsia aldatzea gomendatzen da. Aldaketa hori eskuz egin beharko da, ondoko konfigurazio-elementua aldatuz, urruneko kode-exekuzioa saihesteko:

  <PcVue installation directory>\Bin\PropertyServer.config> fitxategian, "Low" (besterik adierazi ezean, "Full") elementu hau ezarri:

  ```
  <serverProviders>
  <formatter ref="binary" typeFilterLevel="Low" />
  </serverProviders>
  ```

- Firewall-aren konfigurazioa indartzea, dagokion portuan sartzen diren konexioak IISen web zerbitzariaren prozesuaren bidez hasten badira bakarrik baimenduko direla ziurtatuz. Entzuteko portua konfiguragarria da (lehenespenez, 8090), eta baliteke sisteman aldatu izana aplikazioen esploratzailea erabiliz.

Horrez gain, komeni da babes-neurri orokor hauek hartzea, ahultasun horiek ustiatzeko arriskua ahalik eta gehien murrizteko:

- Sareko esposizioa ahalik eta txikiena izatea kontrol gailu eta/edo sistema guztietan, eta Internetetik atzitu ezin direla ziurtatzea.
- Kontrol-sistemak eta urruneko gailuak firewall-en atzean kokatzea eta erakundearen saretik isolatzea.
- Urruneko sarbidea behar denean, metodo seguruak erabili, hala nola sare pribatu birtualak (VPN), VPNek ahultasunak izan ditzaketela eta bertsio berrienean eguneratu behar direla onartuta.

ERREFERENTZIA OSAGARRIAK

- PcVue Solutions - 3 vulnerabilities affect the interface between the Web & Mobile back end and the web services hosted in Microsoft IIS
- KLCERT-20-015: Remote Code Execution in ARC Informatique PcVue
- KLCERT-20-016: Denial-of-Service in ARC Informatique PcVue
- KLCERT-20-017: Session Information Exposure in ARC Informatique PcVue
- ICS Advisory (ICSA-20-308-03) - ARC Informatique PcVue

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?