2019ko Martxoaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Bufferraren gainezkatzea Advantech-en WebAccess-en

Argitalpen data: 2019/03/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- WebAccess

Azalpena:

Larritasun kritikoko ahultasun batek eragiten die Advantech-en WebAcces-en gailuei. Ahultasun hori baliatuz autentifikaziorik gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

- Zerbitzuarekiko interakzioa konfiantzako makinei murriztea.

Xehetasuna:

- Ahultasuna spchapi.exe eta tv_enua.exe exekutagarrietan aurkitzen da, IOCTL 0x2711 deiaren bidez webvrpcs prozesuan. Akatsa gertatzen da luzera finkoko pilan oinarritutako buffer batera kopiatu baino lehen, erabiltzaileak emandako datuen luzeraren baliozkotzea egiten ez delako. Urruneko erasotzaile batek ahultasun hori balia lezake kodea exekutatzeko administratzaile baimenekin.

Etiketak: 0day, Ahultasuna

Cross-site scripting erako ahultasuna PSI GridConnect GmbH-ren gailuetan

Argitalpen data: 2019/03/01

Garrantzia: Handia

Kaltetutako baliabideak:

- Telecontrol Gateway 3G, 4.2.21, 5.0.27, 6.0.16 eta lehenagoko bertsioak
- Telecontrol Gateway XS-MU, 4.2.21, 5.0.27, 5.1.19, 6.0.16 eta lehenagoko bertsioak
- Telecontrol Gateway VM, 4.2.21, 5.0.27, 5.1.19, 6.0.16 eta lehenagoko bertsioak
- Smart Telecontrol Unit TCG, 5.0.27, 5.1.19, 6.0.16 eta lehenagoko bertsioak
- IEC104 Security Proxy, 2.2.10 eta lehenagoko bertsioak

Azalpena:

Can Kurnaz ikertzaileak cross-site scripting (XSS) erako ahultasun bat aurkitu du, PSI GridConnect GmbH-ren hainbat gailuri eragiten diena. Hori baliatuz erasotzaile batek kodea exekuta lezake arbitrarioki xede duen aplikazioan.

Konponbidea:

- PSIk erabiltzaileei aholkatzen die 5.1.20, 6.0.17 bertsioetara eta IEC104 Security Proxy 2.2.11 bertsiora eguneratzea.
- 4.2.x eta 5.0.x bertsioek ez dute zerbitzurik izango

Xehetasuna:

- Web orria sortzean HTML, JavaScript edo VBScript sarreren neutralizazio desegoki baten ondorioz gertatzen den cross-site scripting erako ahultasun bat baliatuz, erasotzaile batek kodea exekuta lezake modu arbitrarioan. Ahultasun horretarako CVE-2019-6528 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Zerbitzuaren ukapena eta kodearen urruneko exekuzioa Rockwell-en RSLinx Classic-en

Argitalpen data: 2019/03/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- RSLinx Classic, v4.10.00 bertsioa eta lehenagokoak.

Azalpena:

Tenablek Rockwell Automationi eman dio bufferraren gainezkatze erako ahultasun baten berri. RSLinx Classic bere gailuei eragiten die eta zerbitzuaren ukapen egoera edo kodearen urruneko exekuzioa eragin litzake.

Konponbidea:

- Ondorengo partxea aplikatzea.

/

Xehetasuna:

- RSLinx Classic-eko dll fitxategi bateko sarrera datuen baliozkotze desegoki baten ondorioz, Open Forward eskaera baten datuak luzera finkoko buffer batera pasatzen direnean, urruneko erasotzaile batek RSLinx.exe aplikazioa gera lezake zerbitzuaren ukapen egoera edo kodearen exekuzioa eraginez. Ahultasun horretarako CVE-2019-6553 identifikatzailea erabili da./li>

Etiketak: Eguneraketa, Ahultasuna

Direktorio jauziaren erako ahultasuna PEPPERL FUCHS-en WirelessHART-Gateways-en

Argitalpen data: 2019/03/07

Garrantzia: Ertaina

Kaltetutako baliabideak:

- WHA-GW-*

Azalpena:

Hamit CIBO ikertzaileak WirelessHART Gateway gailuei eragiten dien direktorio jauziaren erako ahultasun bat aurkitu du. Ahultasun hori baliatuz gero, urruneko erasotzaile ez autentifikatuek fitxategi arbitrarioetara sarbidea lor lezakete.

Konponbidea:

PEPPERL FUCHSek aholkatzen du gailuak eguneratzea ahultasuna konpontzen duen firmwarearen azken bertsiora:

- WHA-GW-*-ETH, 03.00.08 bertsiora
- WHA-GW-*-ETH.EIP, 02.00.01 bertsiora

Xehetasuna:

- Erasotzaile batek ahultasuna balia lezake gailuan gordetzen diren fitxategi eta direktorio murriztuetara sarbidea lortzeko, horietara erreferentzia egiten duten fitxategien parametroak manipulatuz. Sartzen diren eta fcgi-bin/wgsetcgi erabiltzen duten HTTP eskaerek eta fitxategi izenaren parametro batek ahalbidetu lezakete direktorio jauzia. Ahultasun horretarako CVE-2018-16059 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioen eskalatze erako ahultasuna Advantech-en WebAccess-en

Argitalpen data: 2019/03/08

Garrantzia: Ertaina

Kaltetutako baliabideak:

- WebAccess

Azalpena:

Zero Day Initiative-ko Fritz Sands-ek pribilegioen eskalatze erako ahultasun baten berri eman du, Advantech-en WebAccess produktuei eragiten diena. Ahultasun hori arrakastaz baliatuz gero, erasotzaile batek pribilegioak eskalatzea lor lezake.

Konponbidea:

- Une honetan ez dago ahultasun hori konpontzeko partxerik. Zerbitzuarekiko interakzioa konfiantzazko makinei soilik baimentzea aholkatzen da.

Xehetasuna:

- Pribilegioen eskalatze erako ahultasun bat dago sarbidearen kontrolaren barnean produktua instalatzen denean. Instalazio horrek une honetan sistemako fitxategiek duten sarbide kontrolaren murrizpenak ahultzen ditu, eta era berean, fitxategi berriei murrizpen ahulak sartzen dizkie. Erasotzaile batek ahultasun hori balia lezake pribilegioak eskalatzeko administratzaile mailaraino.

Etiketak: 0day, Window

Ispilu atakaren isolamendu desegokia Siemens-en Scalance Xn

Argitalpen data: 2019/03/12

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Scalance X-200 eta X-300, bertsio guztiak
- SCALANCE XP/XC/XF-200, 4.1 bertsioa baino lehenagoko guztiak

Azalpena:

Siemensek ispilu atakaren isolamendu desegoki erako ahultasun bat aurkitu du, ScalanceX switchei eragiten diena. Hori baliatuz, erasotzaile batek informazioa sar lezake sare batean ispilu atakaren bidez, hesiaren monitorizazio funtzioa aktibatuta badu.

Konponbidea:

- Scalance XP/XC/XF-200 produktuen erabiltzaileek 4.1 bertsiora eguneratu behar dute..
- Kaltetutako gainerako produktuen kasuan, Siemensek gomendatzen du sakoneko defentsa printzipioak aplikatzea eta, bereziki, ispilu sarera informazioa bidaltzen duen ezein gailu ez dadila erabilia izan ispilu sarearen barnean.

Xehetasuna:

- Kaltetutako produktuen monitorizazio hesiak ez du modu egokian blokeatzen datuen transmisioa ispilu atakaren bitartez erreplikatutako sarera. Hori baliatuz erasotzaile batek asmo gaiztoko paketeak bidal litzake sare bikoiztuko sistemetara, horrela bere konfigurazioan eta exekuzio denboran eraginez. Ahultasun horretarako CVE-2019-6569 identifikatzailea erreserbatu da.

Etiketak: Komunikazioak, Siemens, Ahultasuna

Hainbat ahultasun Schneider Electric-en produktuetan

Argitalpen data: 2019/03/13

Garrantzia: Handia

Kaltetutako baliabideak:

- VideoXpert OpsCenter, 3.1 bertsioa baino lehenagokoak
- U.motion Builder, 1.3.4 bertsioa

Azalpena:

Bi ikertzailek, RCE Security-ko Julien Ahrens-ek eta Osama Radwan-ek, bilaketa bideko elementu ez kontrolatu eta SQL injekzio erako hainbat ahultasun aurkitu dituzte, Schneider Electric-en hainbat produkturi eragiten dietenak. Urruneko erasotzaile batek DLL liburutegi okerrak dei litzake edo kode arbitrarioa exekutatu.

Konponbidea:

- U.motion Builder-en erabiltzaileek produktua berehala ezabatu behar dute, alboratuta baitago eta ez baitu zerbitzu gehiago jasoko.
- VideoXpert OpsCenter-eko erabiltzaileek 3.1 bertsiora eguneratu behar dute.

Xehetasuna:

- Erasotzaile lokal batek eragin lezake sistemak DLL liburutegi okerrak deitzea. Ahultasun horretarako CVE-2018-7840 identifikatzailea erreserbatu da.
- Urruneko erasotzaile batek, SQL injekzio baten bidez, nahi ez den kodea exekuta lezake sarreretan karaktere desegokiak erabiliz. Ahultasun horretarako CVE-2018-7841 identifikatzailea erreserbatu da.

Etiketak: Scheneider Electric, Ahultasuna

Baldintza ezohikoen egiaztapen desegokia

Schneider Electric-en Triconex TriStation Emulator-en

Argitalpen data: 2019/03/15

Garrantzia: Handia

Kaltetutako baliabideak:

- Triconex TriStation Emulator Version 1.2.0

Azalpena:

Tom Westenberg ikertzaile independenteak baldintza ezohikoen egiaztapen desegoki erako ahultasun bat aurkitu du. Urruneko erasotzaile batek zerbitzuaren ukapena (DoS) exekuta lezake, emuladoreari eraginez.

Konponbidea:

Oraindik ez dago konponbide bat ahultasun horretarako, baina Schneider Electric-ek ondokoa aholkatzen du:

- Kontrol sistemen sareak eta urruneko gailuak suebakien atzean kokatzea eta sare korporatiboetatik isolatzea.
- Kontrol fisiko hobeak ezartzea baimenik gabeko pertsonalak SCIra sarbiderik izan ez dezan.
- Gailu ateragarriak sare isolatu batean eskaneatzea SCI terminal batean erabiliak izan aurretik.
- Urruneko sarbidea behar denean VPN erabiltzea sarearen segurtasun hobea izateko.

Xehetasuna:

- Urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake bereziki diseinatutako pakete bat erabiliz, eta horrela emuladorea blokeatuko luke. Ahultasun horretarako CVE-2018-7803 identifikatzailea erreserbatu da.

Etiketak: Schneider Electric, Ahultasuna

Kontrolatu gabeko bilaketa bideko elementuaren ahultasuna Gemalto-ren Sentinel UltraPro-n

Argitalpen data: 2019/03/15

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Sentinel UltraPro Client Library *ux32w.dll*, 1.3.0, 1.3.1 y 1.3.2 bertsioak.

Azalpena:

Venustech-eko ADLab ikertzaileak kontrolatu gabeko bilaketa bideko elementu erako ahultasun baten berri eman du. Erasotzaile batek kode edo komando arbitrarioak exekuta litzake.

Konponbidea:

- Kaltetutako erabiltzaileek ahultasun hori konpontzen duen 1.3.3 bertsiora eguneratu behar dute.

Xehetasuna:

- Kontrolatu gabeko bilaketa bideko elementu erako ahultasuna baliatuz, erasotzaile batek asmo gaiztoko fitxategi bat karga eta exekuta lezake Sentinel UltraPro-n ux32.dll liburutegitik. Ahultasun horretarako CVE-2019-6534 identifikatzailea erabili da.

Etiketak: Actualización, Vulnerabilidad

Hainbat ahultasun PEPPERL FUCHS-en ecom mugikorretan

Argitalpen data: 2019/03/15

Garrantzia: Handia

Kaltetutako baliabideak:

- i.roc Ci70-Ex
- Cx70-Ex
- CT50-Ex
- Pad-Ex 01
- Tab-Ex 01
- Smart-Ex 01
- Smart-Ex 201
- Ex-Handy 09
- Ex-Handy 209

Azalpena:

Armis-eko Ben Seri-k eta Gregory Vishnepolsky-k Bluetooth komunikazioekin zerikusia duten hainbat eraso bektore aurkitu dituzte eta BlueBorne ahultasuna argitaratu dute. Erasotzaile batek gailuaren kontrola har lezake eta kode arbitrarioa exekutatu edo datu

sentikorretara sarbidea lortu.

Konponbidea:

PEPPERL FUCHSek gailuak eguneratzea gomendatzen du, kaltetuta dagoenaren arabera, dagokion firmwarearekin:

- CT50-Ex Android, Smart-Ex 01 eta Smart-Ex 201: FOTA-Update
- CT50-Ex Windows eta Pad-Ex 01: Microsoft Update

Xehetasuna:

- Autentifikaziorik gabeko urruneko erasotzaile batek gailuari edo erabiltzaileari buruzko informazio pribatua eskura lezake, kode arbitrarioa exekutatu edo man-in-the-middle (MitM) eraso bat egin. Ahultasun horietarako honako identifikatzaileak erabili dira CVE-2017-0781, CVE-2017-0785, CVE-2017-0782, CVE-2017-0783 eta CVE-2017-8628.

Etiketak: Komunikazioak, Mugikorrak, Ahultasuna

Hainbat ahultasun ENDRESS HAUSER-en Field Xpert-en

Argitalpen data: 2019/03/20

Garrantzia: Handia

Kaltetutako baliabideak:

- PDA Field Xpert SFX350 eta SFX370.
- Ekipoak konfiguratzeko Tablet PC Field Xpert SMT70.

Azalpena:

imec-DistriNet-eko Mathy Vanhoef ikertzaileak wifia gaitua dutenean Field Xpert de Endress Hauser gailuei eragiten dieten hainbat ahultasunen berri eman du. Horiek baliatuz erasotzaile batek paketeen erreprodukzio, deszifratze eta faltsutze erasoak egin litzake wifiaren eragin eremuaren barnean.

Konponbidea:

- Windows Mobile erabiltzen duten Field Xpert SFX350 eta SFX370 gailuen kasuan, Endress Hauser-ek aholkatzen du Microsoft-ek eskainitako azken segurtasun eguneraketa ezartzea (SR18012500_802T_Cx70_WM65_ALL.CAB).
- Windows 10 Pro 1703 64 EN erabiltzen duen Field Xpert SMT70 gailuaren kasuan, Endress Hauser-ek aholkatzen du eskuragarri dagoen Windowsen azken bertsiora eguneratzea.

Xehetasuna:

- WPA2 estandarraren barnean hainbat ahultasun aurkitu dira. Horiek baliatuz erasotzaile batek PTK (Pairwise Transient Key) aldi baterako gakoa, talde gako bat edo haririk gabeko bezero batean edo urruneko sarbideko puntu batean integritate gako bat berrinstala litzake. Horrela paketeak deszifratu edo injekta litzake man-in-the-middle erasoen bidez sarbide puntuaren eta bezeroaren artean. Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087 eta CVE-2017-13088.

Etiketak: Komunikazioak, Ahultasuna

Hainbat ahultasun Medtronic-en Conexus telemetria protokoloan

Argitalpen data: 2019/03/22

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- MyCareLink Monitor, 24950 eta 24952 bertsioak
- CareLink Monitor, 2490C bertsioa
- CareLink 2090 Programmer
- Amplia CRT-D, Claria CRT-D, Compia CRT-D, Concerto CRT-D, Concerto II CRT-D, Consulta CRT-D, Evera ICD, Maximo II CRT-D eta ICD, Mirro ICD, Nayamed ND ICD, Primo ICD, Protecta ICD eta CRT-D, Secura ICD, Virtuoso ICD, Virtuoso II ICD, Visia AF ICD eta Viva CRT-D, modelo guztiak.

Azalpena:

Clever Security-ko Peter Morgan-ek, KU Leuven-eko Dave Singelée eta Bart Preneel-ek, lehen KU Leuven-ekoa zen eta une honetan University of Birmingham-ekoa den Eduard Marin-ek, University of Birmingham-eko Flavio D. Garcia-k etaTom Chothia-k eta University Hospital Gasthuisberg Leuvenha-ko Rik Willems-ek hainbat ahultasunen berri eman dute, Medtronic-en Conexus telemetria protokoloari eragiten diotenak. Kaltetutako produkturen batera gertuko sarbidea lukeen erasotzaile batek Conexus telemetria sistemaren irrati-maiztasuneko (IM) komunikazioa interferitu, sortu, aldatu edo atzeman lezake. Horrela produktuaren funtzionalitateei eragingo lieke eta transmititutako datu konfidentzialetara sarbidea lor liteke.

Konponbidea:

Medtronic-ek monitorizazio eta erantzun kontrol osagarriak ezarri dizkie kaltetutako gailuek egiten dituzten protokoloaren erabilera desegokiei. Horrez gain, arintze berriak prestatzen ari da, etorkizuneko eguneraketetan jasoko direnak. Medtronic-ek ondoko neurriak hartzea ere gomendatzen du:

- Programatzaileen eta monitoreen gaineko kontrol fisikoa izatea.
- Medtronic-etik edo osasun produktuen zure hornitzailearengandik zuzenean eskuratutako programatzaile, monitore eta gailu

ezargarriak soilik erabiltzea.
- Programatzaile eta monitoreetara gailu desegokiak ez konektatzea eskuragarri dauden USB ataken bidez.
- Programatzaileak ingurune fisikoki kontrolatuetan soilik erabiltzea, adibidez ospitale eta klinika baimenduetan.
- Ohiz kanpoko edozein portaerari buruz informatzea.

Xehetasuna:

- Conexus telemetria protokoloak ez du inplementatzen autentifikazioa eta baimena. Kaltetutako produktu batera irispide laburreko sarbidea lukeen erasotzaile batek datuak injektatu, erreproduzitu, aldatu eta atzeman litzake telemetriaren komunikazioaren barnean, bai eta ezarritako gailu kardiakoan memoria aldatu ere. Ahultasun horretarako CVE-2019-6538 identifikatzailea erreserbatu da.
- Conexus telemetria protokoloak ez du inplementatzen zifratua. Kaltetutako produktu batera irispide laburreko sarbidea lukeen erasotzaile batek komunikazioak entzun litzake, datu konfidentzialen transmisioa barne. Ahultasun horretarako CVE-2019-6540 identifikatzailea erreserbatu da.

Etiketak: 0day, Komunikazioak, Ahultasuna

Hainbat ahultasun Phoenix Contact gailuetan

Argitalpen data: 2019/03/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- RAD-80211-XD (2885728)
- RAD-80211-XD/HP-BUS (2900047)
- FL NAT SMN 8TX-M (2702443)
- FL NAT SMN 8TX-M-DMG (2989352)
- FL NAT SMN 8TX (2989365)
- FL NAT SMCS 8TX (2989378)

Azalpena:

Maxim Rupp segurtasun ikertzaileak Phoenix Contact-i bi ahultasunen berri eman dio, bata larritasun kritikokoa eta bestea altukoa. Horiek baliatuz baimenik gabeko erasotzaile batek gailura sarbidea lor lezake, edo komandoak injekta litzake administratzaile pribilegioekin.

Konponbidea:

Phoenix Contact-ek aholkatzen du gailuak sare kontrolatuetan eta suebakiez babestuta daudenetan erabiltzea. Kaltetutako gailuaren arabera:

- RAD-80211-XD eta RAD-80211-XD/HP-BUS gailuak: zerbitzurik ez daukate dagoeneko, beraz ez dute jasoko ahultasuna arintzeko eguneraketarik. Phoenix Contact-ek aholkatzen du kaltetutako gailuak ordeztea.
- FL NAT gailuak: erasotzaile batek gailura arrakastaz sartzea lortuko balu, ondokoa aholkatzen da:
    - Administrazio lanen ondoren web interfazearen saioa berehala ixtea.
    - Web interfazea desgaitzea eta sarbidearen konfigurazioa SNMP bidez erabiltzea.

Xehetasuna:

- Larritasun kritikoko ahultasuna WebHMI utilitatean dago. Edozein erabiltzailek balia lezake ahultasun hori gailuan komandoak exekutatzeko administratzaile pribilegioekin. Ahultasun horretarako CVE-2019-9743 identifikatzailea erreserbatu da.
- Kritikotasun altuko ahultasuna saioa hastean dago. Jatorriko IP helbidea saioaren identifikatzaile modura erabiltzen da, eta IP helbide berdina duten erabiltzaileek web interfazera sarbide osoa eskura lezakete. Ahultasun horretarako CVE-2019-9744 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Autentifikazio eza ENTTEC-en argiztapen kontrolatzaileetan

Argitalpen data: 2019/03/27

Garrantzia: Handia

Kaltetutako baliabideak:

- Datagate MK2, 70044_update_05032019-482 firmwarearen aurreko bertsio guztiak.
- Storm 24, 70050_update_05032019-482 firmwarearen aurreko bertsio guztiak.
- Pixelator, 70060_update_05032019-482 firmwarearen aurreko bertsio guztiak.

Azalpena:

NewSky Security-ko Ankit Anubhav ikertzaileak funtzio kritikoan autentifikazio gabezia erako ahultasun baten berri eman du, ENTTECen argiztapen kontrolatzaileei eragiten diena. Hori baliatuz urruneko erasotzaile batek gailua berrabiaraz lezake, eta horrela zerbitzuaren ukapen egoera eragin.

Konponbidea:

ENTTECek erabiltzaileei aholkatzen die 2019ko martxoko revB firmware bertsiora edo ondorengoetara eguneratzea. Ondoko loturetatik deskarga daiteke:

- Datagate MK2 70044_update_05032019-482
- Storm 24 70050_update_05032019-482
- Pixelator 70060_update_05032019-482

Xehetasuna:

- Baimenik gabeko erasotzaile batek gailuaren berrabiatzea eragin lezake urrunetik, zerbitzuaren ukapen egoera eraginez. Ahultasun horretarako CVE-2019-6542 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna.

Zerbitzuaren ukapena Rockwell Automation-en CA PowerFlex 525-en aldatzaileetan

Argitalpen data: 2019/03/29

Garrantzia: Handia

Kaltetutako baliabideak:

- EtherNet/IP ataka barneratuta duten CA PowerFlex 525-en aldatzaileak, 5.001 eta lehenagoko bertsioak.

Oharra: CA PowerFlex 525-en aldatzaileekin bateragarriak diren 25-COMM-E2P Dual-Port EtherNet/IP aldatzaileei ez die eragiten ahultasun honek.

Azalpena:

Applied Risk-eko Nicolas Merle ikertzaileak kontrolatu gabeko baliabideen kontsumo erako ahultasun bat aurkitu du, Rockwell Automation-en CA PowerFlex 525-en aldatzaileei eragiten diena. Urruneko erasotzaile batek baliabideak agortu litzake zerbitzuaren ukapen egoera eraginez, edo memoria honda lezake.

Konponbidea:

- Kaltetutako gailuak 5.002 edo geroagoko firmwarearekin eguneratzea.

Xehetasuna:

- Autentifikaziorik gabeko urruneko erasotzaile batek, CIP pakete berezien hurrenez hurreneko bidalketaren bidez, zerbitzuen ukapen egoera edota memoriaren hondatzea eragin litzake kaltetutako produktuan. Ahultasun horretarako CVE-2018-19282 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna.

Sarbidearen kontrol desegokia Advantech-en WebAccess-en

Argitalpen data: 2019/03/29

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- WebAccess

Azalpena:

Trend Micro Zero Day Initiative-ko Mat Powell ikertzaileak sarbidearen kontrol desegoki erako bi ahultasunen berri eman du, Advantech-en WebAccess softwareari eragiten diotenak. Urruneko erasotzaile batek gailuan kode arbitrarioa exekutatzea lor lezake autentifikatuta egon gabe.

Konponbidea:

- Ez da konponbiderik argitaratu ahultasun hauetarako. Interakzioa konfiantzako makinek soilik izatea gomendatzen da. WebAccess-erako komunikazioa soilik baimendu behar zaie prozesuarekin harremana zilegi den moduan duten bezeroei eta zerbitzariei.

Xehetasuna:

- Erabiltzaileak emandako testu katearen egiaztapen eza antzeman da spchapi.exe eta tv_enua.exe zerbitzuetan, sistemari egiten zaion dei bat exekutatzeko erabili aurretik. Autentifikaziorik gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake Administratzailearen testuinguruan.

Etiketak: 0day, Ahultasuna.