2021ko Martxoaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

---

fdtContainer sistemaren ahultasun batek ENDRESS HAUSER erakundearen hainbat produkturi eragin die

Argitalpen data: 2021/03/01

Garrantzia: Altua

Kaltetutako baliabideak:

- DeviceCare SFE100, 1.07.00 bertsioa eta aurrekoak;
- Field Xpert SMTxx (Software SFE300), 1.05.00 bertsioa eta aurrekoak;
- FieldCare SFE500, 2.15.01 bertsioa eta aurrekoak;
- Asset Health Monitoring SRP700 (Software FieldCare SFE500), 2.15.01 bertsioa (FieldCare SFE500) eta aurrekoak.

Azalpena:

M&M Software GmbH erakundeak larritasun handiko ahultasun baten berri eman du, erakundeak koordinatua. Horren bidez, erasotzaile batek kode maltzurra exekuta lezake.

Konponbidea:

Konponbide bat izan arte, honako arintze-neurriak hartzea gomendatzen da:

- Proiektuaren datuak partekatzea, partekatze-seguruaren zerbitzuen bidez soilik;
- Proiektuaren biltegiratzea baimenik gabeko manipulazioetatik babesteko baliabide egokiak erabiltzea;
- Proiektuaren datuak iturri ezezagun batetik ez irekitzea;
- Aplikazio anfitrioiaren erabiltzaile eskubideak gutxienekora murriztea.

Xehetasunak:

Datu ez fidatzekoen deserializazio motako ahultasun baten ondorioz (fdtContainer osagaian), erasotzaile batek kode maltzurra exekuta lezake, host-aren aplikazioa exekutatzen den lan-estaziotik, aplikazio horren erabiltzaile-baimenekin. INCIBE-CERT sisteman argitaratu den ahultasun horretarako CVE-2020-12525 identifikatzailea esleitu da.

Etiketak: Azpiegitura kritikoak, Ahultasuna

Sarbide desegokiko balioztatzea Rockwell Automation erakundearen hainbat produktutan

Argitalpen data: 2021/03/03

Garrantzia: Ertaina

Kaltetutako baliabideak:

Rockwell Automation erakundearen gailu-bertsio hauek kaltetuta daude:

- Armor Compact GuardLogix 5370 kontrolagailuak, 33 bertsioa eta aurrekoak;
- Armor GuardLogix segurtasun-kontrolagailuak, 33 bertsioa eta aurrekoak;

- CompactLogix 5370 L1 kontrolagailuak, 33 bertsioa eta aurrekoak;
- CompactLogix 5370 L2s, kontrolagailuak, 33 bertsioa eta aurrekoak;
- CompactLogix 5370 L3 kontrolagailuak, 33 bertsioa eta aurrekoak;
- Compact GuardLogix 5370 kontrolagailuak, 33 bertsioa eta aurrekoak;
- ControlLogix 5570 kontrolagailuak, 33 bertsioa eta aurrekoak.

Azalpena:

Yeop Chang ikertzaileak tarteko larritasuneko ahultasun baten berri eman du, sarbide desegokiaren balioztatze motakoa. Horren ondorioz, Rockwell Automation erakundearen kontroladore asko kaltetu litezke.

Konponbidea:

Rockwell Automation erakundeak kaltetutako erabiltzaileei firmwarea eguneratzea gomendatu die, 33.011 bertsiora edo osteko batera.

Xehetasunak:

Konexioa ezartzeko algoritmoak, CompactLogix 5370 eta ControlLogix 5570 sistemek erabilia, ez du ondo kudeatzen kontrol-fluxua exekuzioan, eta bukle edo begizta infinitua sortzen du. Horren ondorioz, erasotzaile batek CIP paketeen eskaerak bidal ditzake (Common Industrial Protocol), bereziki diseinatuta, kontroladore batera, eta beste produktuekiko komunikazioen zerbitzuan ukapen baldintzak eragin. Ahultasun horretarako, CVE-2020-6998 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Hitachi ABB Power Grids erakundearen Ellipse EAM sisteman

Argitalpen data: 2021/03/03

Garrantzia: Ertaina

Kaltetutako baliabideak:

Ellipse Enterprise Asset Management (EAM), 9.0.25 bertsioa eta aurrekoak.

Azalpena:

Hitachi ABB Power Grids erakundeak tarteko larritasuneko bi ahultasunen berri eman dio CISAri. Horien bidez, erasotzaile batek informazio konfidentziala ostu lezake, erabiltzaile-saioa bahitu, edota egiaztatze-kredentzialak konprometitu.

Konponbidea:

9.0.26 bertsiora eguneratzea.

Xehetasunak:

- XSS (Cross Site Scripting) ahultasun baten bidez, erasotzaile batek erabiltzaile bat engainatu lezake kode maltzurra duen lotura batera sartzeko. Hori web nabigatzailean exekutatuko litzateke, eta erasotzaileak informazio konfidentziala konprometitu edota erabiltzailearen saioa bahitu lezake. Ahultasun horretarako, CVE-2021-27416 identifikatzailea esleitu da.
- clickjacking motako ahultasun baten bidez, erasotzaile batek erabiltzaile bat engainatu lezake webgune bat bisitatzeko eta Ellipse aplikazioaren saio-hasieraren interfaze bat simulatzeko. Horrela, erabiltzailearen kredentzialak konprometituko lituzke. Ahultasun horretarako CVE 2021-27414 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Alboko kanaleko ahultasuna Bosch produktu batzuetan

Argitalpen data: 2021/03/04

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Bosch AUTODOME 700 IP IVA hemen: CPP3;
- Bosch AUTODOME 7000 series hemen: CPP4;
- Bosch AUTODOME 800 hemen: CPP3;
- Bosch AUTODOME Easy II IP series hemen: CPP3;
- Bosch AUTODOME IP 4000 HD hemen: CPP4;
- Bosch AUTODOME IP 4000i hemen: CPP7.3;
- Bosch AUTODOME IP 5000 HD hemen: CPP4;
- Bosch AUTODOME IP 5000 hemen: CPP4;
- Bosch AUTODOME IP 5000i hemen: CPP7.3;
- Bosch AUTODOME IP starlight 5000i (IR) hemen: CPP7.3;
- Bosch AUTODOME IP starlight 7000i hemen: CPP7.3;
- Bosch AUTODOME Junior 800 hemen: CPP3;
- Bosch AUTODOME Junior HD, Jr HD fix hemen: CPP3;

- Bosch DINION 2X, NBN-498-P hemen: CPP3;
- Bosch DINION HD 1080p hemen: CPP4;
- Bosch DINION HD 1080p HDR hemen: CPP4;
- Bosch DINION HD 720p hemen: CPP4;
- Bosch DINION IP 3000i hemen: CPP7.3;
- Bosch DINION IP 4000 HD hemen: CPP4;
- Bosch DINION IP 5000 HD hemen: CPP4;
- Bosch DINION IP 5000 MP hemen: CPP4;
- Bosch DINION IP bullet 4000 hemen: CPP4;
- Bosch DINION IP bullet 4000i hemen: CPP7.3;
- Bosch DINION IP bullet 5000 hemen: CPP7.3;
- Bosch DINION IP bullet 5000 hemen: CPP4;
- Bosch DINION IP bullet 5000i hemen: CPP7.3;
- Bosch DINION IP bullet 6000i hemen: CPP7.3;
- Bosch DINION IP starlight 6000 hemen: CPP7;
- Bosch DINION IP starlight 7000 hemen: CPP7;
- Bosch DINION IP starlight 7000 HD hemen: CPP4;
- Bosch DINION IP starlight 8000 12MP hemen: CPP6;
- Bosch DINION IP thermal 8000 hemen: CPP7;
- Bosch DINION IP thermal 9000 RM hemen: CPP7;
- Bosch DINION IP ultra 8000 12MP hemen: CPP6;
- Bosch DINION IP ultra 8000 12MP C/CS monturadun teleobjektiboarekin hemen: CPP6;
- Bosch DINION XF 720p , NBN-921-P hemen: CPP3;
- Bosch DINION XF, NBC-455-P hemen: CPP3;
- Bosch DINION imager 9000 HD hemen: CPP4;
- Bosch EXTEGRA IP dynamic 9000 hemen: CPP4;
- Bosch EXTEGRA IP starlight 9000 hemen: CPP4;
- Bosch Economic versión VIP-X1XF-E hemen: CPP3;
- Bosch Economy Box Cameras, NBC-225 series, NBC-255 series, NTC-255-PI hemen: CPP3;
- Bosch Economy Dome Cameras, NDC-225 series, NDC-255 series hemen: CPP3;
- Bosch Economy HD Box Cameras, NBC-265 series, NTC-265-PI hemen: CPP3;
- Bosch Economy HD Dome Cameras, NDC-265 series, NDN-265-PIO hemen: CPP3;
- Bosch Extreme series EX30 IR, NEI-30 IR Imager hemen: CPP3;
- Bosch FLEXIDOME 2X, NDN-498-P hemen: CPP3;
- Bosch FLEXIDOME HD 1080p hemen: CPP4;
- Bosch FLEXIDOME HD 1080p HDR hemen: CPP4;
- Bosch FLEXIDOME HD 720p hemen: CPP4;
- Bosch FLEXIDOME IP 3000i hemen: CPP7.3;
- Bosch FLEXIDOME IP 4000i hemen: CPP7.3;
- Bosch FLEXIDOME IP 5000i hemen: CPP7.3;
- Bosch FLEXIDOME IP indoor 4000 HD hemen: CPP4;
- Bosch FLEXIDOME IP indoor 4000 IR hemen: CPP4;
- Bosch FLEXIDOME IP indoor 5000 HD hemen: CPP4;
- Bosch FLEXIDOME IP indoor 5000 MP hemen: CPP4;
- Bosch FLEXIDOME IP micro 2000 HD hemen: CPP4;
- Bosch FLEXIDOME IP micro 2000 IP hemen: CPP4;
- Bosch FLEXIDOME IP micro 5000 HD hemen: CPP4;
- Bosch FLEXIDOME IP micro 5000 MP hemen: CPP4;
- Bosch FLEXIDOME IP outdoor 4000 HD hemen: CPP4;
- Bosch FLEXIDOME IP outdoor 4000 IR hemen: CPP4;
- Bosch FLEXIDOME IP outdoor 5000 HD hemen: CPP4;
- Bosch FLEXIDOME IP outdoor 5000 MP hemen: CPP4;
- Bosch FLEXIDOME IP panoramic 5000 hemen: CPP4;
- Bosch FLEXIDOME IP panoramic 6000 12MP 180 hemen: CPP6;
- Bosch FLEXIDOME IP panoramic 6000 12MP 180 IVA hemen: CPP6;
- Bosch FLEXIDOME IP panoramic 6000 12MP 360 hemen: CPP6;
- Bosch FLEXIDOME IP panoramic 6000 12MP 360 IVA hemen: CPP6;
- Bosch FLEXIDOME IP panoramic 7000 12MP 180 hemen: CPP6;
- Bosch FLEXIDOME IP panoramic 7000 12MP 180 IVA hemen: CPP6;
- Bosch FLEXIDOME IP panoramic 7000 12MP 360 hemen: CPP6;
- Bosch FLEXIDOME IP panoramic 7000 12MP 360 IVA hemen: CPP6;
- Bosch FLEXIDOME IP starlight 5000i (IR) hemen: CPP7.3;
- Bosch FLEXIDOME IP starlight 6000 hemen: CPP7;
- Bosch FLEXIDOME IP starlight 7000 hemen: CPP7;
- Bosch FLEXIDOME IP starlight 8000i hemen: CPP7.3;
- Bosch FLEXIDOME XF 720p , NDN-921-P hemen: CPP3;
- Bosch FLEXIDOME XF, NDC-455-P hemen: CPP3;
- Bosch FLEXIDOME corner 9000 MP hemen: CPP4;
- Bosch Far Infra-Red camera, VOT-320 hemen: CPP3;
- Bosch IP bullet 4000 HD hemen: CPP4;
- Bosch IP bullet 5000 HD hemen: CPP4;
- Bosch IP micro 2000 hemen: CPP4;
- Bosch IP micro 2000 HD hemen: CPP4;
- Bosch MIC IP PSU hemen: CPP3;
- Bosch MIC IP dynamic 7000 hemen: CPP4;
- Bosch MIC IP fusion 9000i hemen: CPP7.3;
- Bosch MIC IP starlight 7000 hemen: CPP4;
- Bosch MIC IP starlight 7000i hemen: CPP7.3;
- Bosch MIC IP starlight 7100i hemen: CPP7.3;
- Bosch MIC IP ultra 7100i hemen: CPP7.3;
- Bosch REG 1.5 IP y REG L2 hemen: CPP3;
- Bosch TINYON IP 2000 family hemen: CPP4;
- Bosch VG4 AUTODOME IP series hemen: CPP3;
- Bosch VG5 AUTODOME IP series hemen: CPP3;
- Bosch VIDEOJET connect 7000, VJC-7000 hemen: CPP-ENC;
- Bosch VIDEOJET decoder 3000, VJD-3000 hemen: CPP-ENC;
- Bosch VIDEOJET multi 4000 hemen: CPP5;

- Bosch VIP X1 XF Single-Channel H.264 Encoder hemen: CPP3;
- Bosch VIP-X1600-XFM4 hemen: CPP-ENC;
- Bosch VIP-X16XF-E hemen: CPP5;
- Bosch VJT-X20/X40XF-E hemen: CPP-ENC;
- Bosch VJT-XTCXF hemen: CPP-ENC;
- Bosch Vyal-proof FLEXIDOME HD 1080p hemen: CPP4;
- Bosch Vyal-proof FLEXIDOME HD 1080p HDR hemen: CPP4;
- Bosch Vyal-proof FLEXIDOME HD 720p hemen: CPP4;
- Bosch Video Conference Dome IVA hemen: CPP3;
- Bosch WLAN cameras NBC-255-W eta NBC-265-W hemen: CPP3.

Azalpena:

Ahultasuna Victor Lomne eta Thomas Roche segurtasun-ikertzaileek antzeman zuten, eta NXP erakundeak eman zion Bosch enpresari horren berri. Larritasun-maila tartekoa da, eta alboko kanaleko eraso motan oinarritzen da (side channel), ECDSA (Elliptic Curve Digital Signature Algorithm) gako pribatuak erauzteko.

Konponbidea:

Txip ahula ezin da eguneratu, ez dago konponbide posiblerik, beraz, ondoren zehaztutako neurriak planteatu behar dira:

- ECDSA klabeen ordez RSA klabeak jartzea,
- Galdutako gailu bati dagozkion gakoak dagokion CA bidez eta ziurtagiriaren ezeztatze informazioaren bidez baliogabetu behar dira,
- Kamera erabiltzeari utzi aurretik, ezabatu egin behar dira gauzak,
- Kamera modeloak CPP13 eta CPP14ra eguneratzea, jada ez baitute txip ahulik erabiltzen.

Xehetasunak:

Uhin elektromagnetikoen alboko kanaleko ahultasun bat antzeman da NXP SmartMX/P5x segurtasun-mikrokontrolagailuen eta A7x egiaztatze seguruko mikrokontrolagailuetan, CryptoLib sistemarekin, 2.9. bertsiora arte. Ahultasun horren bidez, erasotzaile batek ECDSA gako pribatua erauzi lezake txipera fisikoki sartu ostean. Ahultasun horretarako, CVE-2021-3011 identifikatzailea esleitu da.

Etiketak: Komunikazioa, Azpiegitura kritikoak, IoT, Ahultasuna.

Mugetatik kanpoko idazketa Dräger produktuetan

Argitalpen data: 2021/03/04

Garrantzia: Altua

Kaltetutako baliabideak:

- CC-Vision Basic, 7.5.2 bertsioa eta aurrekoak;
- CC-Vision E-Cal, 7.2.4.8 bertsioa eta aurrekoak.

Azalpena:

Mario Ceballos ikertzaileak DrÃ¤ger erakundeari larritasun handiko ahultasun baten berri eman dio. Horren bidez, erasotzaile batek kode maltzurra exekutatu edo sistema blokeatu lezake.

Konponbidea:

Eguneratzea:

- CC-Vision Basic 7.5.3 bertsiora edo osteko batera;
- CC-Vision E-Cal 7.2.5.0 bertsiora edo osteko batera.

Xehetasunak:

Mugetatik kanpoko idazketaren motako ahultasun baten ondorioz, bufferraren gainezkatzea eragin lezakeena, erasotzaile batek kode maltzurra exekuta lezake, edo sistema blokeatu, gdt artxiboak kargatu edo irekitzean.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Siemens segurtasun oharrak, 2021eko martxoa

Argitalpen data: 2021/03/09

Garrantzia: Altua

Kaltetutako baliabideak:

- Solid Edge SE2020, bertsio guztiak;
- Solid Edge SE2021, bertsio guztiak;
- SIMATIC S7-PLCSIM V5.4, bertsio guztiak;
- RUGGEDCOM RM1224, 6.3 bertsioa;
- SCALANCE M-800, 6.3 bertsioa;
- SCALANCE S615, 6.3 bertsioa;
- SCALANCE SC-600, 2.1 edo osteko bertsio guztiak, baina 2.1.3ren aurrekoak;

- PLUSCONTROL 1st Gen, bertsio guztiak;
- SENTRON 3VA COM100/800, bertsio guztiak;
- SENTRON 3VA DSP800, CVE-2020-17437 kodeak soilik eragindako bertsio guztiak;
- SENTRON PAC2200 (CLP Approval), CVE-2020-17437 kodeak soilik eragindako bertsio guztiak;
- SENTRON PAC2200 (con MID Approval), CVE-2020-17437 kodeak soilik eragindako bertsio guztiak;
- SENTRON PAC2200 (sin MID Approval), CVE-2020-17437 kodeak soilik eragindako bertsio guztiak;
- SENTRON PAC3200, 2.4.7 bertsioaren aurreko guztiak;
- SENTRON PAC3200T, CVE-2020-17437 kodeak soilik eragindako bertsio guztiak;
- SIMATIC MV400 family, 7.0.6 bertsioaren aurreko guztiak;
- Solid Edge SE2020, SE2020MP13 bertsioaren aurreko guztiak;
- Solid Edge SE2021, SE2021MP3 bertsioaren aurreko guztiak;
- Solid Edge SE2021, soilik CVE-2020-28385 eta CVE-2021-27380 kodeek eragindako SE2021MP3 bertsioa;
- SINEMA Remote Connect Server, 3.0ren aurreko bertsio guztiak;
- LOGO! 8 BM (SIPLUS aldagaiak barne), bertsio guztiak;
- SCALANCE SC600 Family, 2.0ren aurreko bertsio guztiak;
- SIMATIC NET CM 1542-1, bertsio guztiak;
- RUGGEDCOM RM1224, 4.3 bertsioa eta osteko guztiak;
- SCALANCE M-800, 4.3 bertsioa eta osteko guztiak;
- SCALANCE S615, 4.3 bertsioa eta osteko guztiak;
- SCALANCE SC-600 Family, 2.0 bertsioa edo ostekoak, baina 2.1.3ren aurrekoak;
- SCALANCE X300WG, 4.1en aurreko bertsio guztiak;
- SCALANCE XM400, 6.2ren aurreko bertsio guztiak;
- SCALANCE XR500, 6.2ren aurreko bertsio guztiak;
- SCALANCE Xx200 Family, 4.1en aurreko bertsio guztiak.

Azalpena:

Siemensek produktu batzuen inguruan hainbat segurtasun-eguneratze argitaratu ditu, bere hileroko jakinarazpenean.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneratzeak Siemens deskarga paneletik deskargatu daitezke. Eguneratzerik gabeko produktuetarako, Erreferentzien atalean azaldutako arintze-neurriak aplikatu behar dira.

Xehetasunak:

Siemensek, segurtasun partxeei buruzko hileroko jakinarazpenean, 25 segurtasun-abisu eman ditu; horietatik 13 eguneratzeak dira.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Mugetatik kanpoko irakurketa,
- Mugetatik kanpoko idazketa,
- Puntero ez fidagarriaren erreferentzia galtzea,
- Direktorio mugatu baterako ibilbide-izenaren (path traversal) mugatze ez zuzena,
- Erabiltzaile interfazean eragiketa arriskutsuen inguruan behar bezala ez ohartaraztea,
- Bukle infinitua,
- Zerbitzua ukatzea,
- Behar besteko aleatoriotasunik gabeko TCP konexioen balioak ISN delakoetan (Initial Sequence Numbers).
- Sartzen diren TCP RST paketeen balioztatze desegokia,
- XML Eternal Entity Reference (XXE) mugatze desegokia,
- Baimen okerra,
- Salbuespen-baldintzen kudeaketa ez zuzena,
- Pilan oinarritutako buffer gainezkatzea (stack).

Ahultasun horietarako, honako identifikatzaileak erreserbatu dira: CVE-2021-22643, CVE-2021-22645, CVE-2021-22647, CVE-2021-22649, CVE-2021-22651, CVE-2021-25673, CVE-2021-25674, CVE-2021-25675, CVE-2021-25676, CVE-2020-28388, CVE-2020-13987, CVE-2020-17437, CVE-2020-25241, CVE-2020-27632, CVE-2020-28385, CVE-2020-28387, CVE-2021-27380, CVE-2021-27381, CVE-2020-25239, CVE-2020-25240, CVE-2020-25236, CVE-2019-3823 eta CVE-2021-25667.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Siemens, Ahultasuna.

Schneider Electric erakundearen produktuen ahultasunak

Argitalpen data: 2021/03/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- ION8650, 4.40.1 bertsioaren aurreko guztiak;
- ION8800, 372 bertsioaren aurreko guztiak;
- ION7650 (Hardware rev. 4 edo aurrekoak), 376 bertsioaren aurreko guztiak;
- ION7650 (Hardware rev. 5 edo aurrekoak), 416 bertsioaren aurreko guztiak;
- ION7700/73xx, bertsio guztiak;
- ION83xx/84xx/85xx/8600, bertsio guztiak;
- ION7400, 3.0.0 bertsioaren aurreko guztiak;
- ION9000, 3.0.0 bertsioaren aurreko guztiak;
- PM8000, 3.0.0 bertsioaren aurreko guztiak;
- IGSS Definition (Def.exe), 15.0.0.21041 bertsioa eta aurrekoak.

Azalpena:

Schneider Electric erakundeak hainbat ahultasun argitaratu ditu; horien bidez, neurgailua berrabiaraz liteke, kodea urrunetik exekutatu, datuen irakurketa edo idazketa arbitrarioa burutu, edo datuak galdu litezke.

Konponbidea:

Eguneratzea:

- ION8650, V4.40.1;
- ION8800, V372;
- ION7650 (Hardware rev. 4 edo aurrekoa), V376;
- ION7650 (Hardware rev. 5), V416;
- ION7700/73xx, euskarririk gabe. Fabrikatzailearen gomendioa: modelo berriren batengatik ordeztea (PowerLogic ION9000, PowerLogic PM8000, edo PowerLogic ION7400);
- ION83xx/84xx/85xx/8600, euskarririk gabe. Fabrikatzailearen gomendioa: modelo berriren batengatik ordeztea (PowerLogic ION8650);
- ION7400, V3.0.0;
- ION9000, V3.0.0;
- PM8000, V3.0.0;
- IGSS Definition (Def.exe), 15.0.0.21042 bertsioa.

Xehetasunak:

- Memoriaren bufferraren mugen barruko eragiketa-mugatze desegokiaren ondorioz, neurgailua berrabiarazi egin liteke, edo kodearen urruneko exekuzioa burutu. Ahultasun horietarako CVE-2021-22713 eta CVE-2021-22714 identifikatzaileak erreserbatu dira.
- Memoriaren bufferraren mugen barruko eragiketa-murrizketa desegokiaren ondorioz, datuak galdu litezke, edo kodearen urruneko exekuzioa burutu, CGF (Configuration Group File) artxibo maltzur bat IGSS Definition-era inportatzen denean. Ahultasun horietarako CVE-2021-22709 eta CVE-2021-22710 identifikatzaileak erreserbatu dira.
- Memoriaren bufferraren mugen barruko eragiketa-murrizketa desegokiaren ondorioz, idazketa edo irakurketa arbitrarioaren baldintza eman liteke, CGF (Configuration Group File) artxibo maltzur bat IGSS Definition-era inportatzen denean. Ahultasun horietarako CVE-2021-22711 eta CVE-2021-22712 identifikatzaileak erreserbatu dira.

Etiketak: Eguneratzea, Azpiegitura kritikoak, SCADA, Schneider Electric, Ahultasuna.

RCE ahultasuna Fatek Automation erakundearen PLC WinProladder sisteman

Argitalpen data: 2021/03/12

Garrantzia: Altua

Kaltetutako baliabideak:

Fatek Automation PLC WinProladder.

Azalpena:

Francis Provencher {PRL} ikertzaileak, Trend Microko ZDIrekin elkarlanean, kodearen urruneko exekuzio (RCE) motako 0day ahultasun baten berri eman du. Larritasun handikoa da, eta Fatek Automation erakundearen PLC WinProladder sistemari eragiten dio.

Konponbidea:

Ahultasun hori partxerik gabe zabaldu da publikoki, ICS-CERT erakundearen akordioarekin, beraz, gomendatutako neurri bakarra aplikazioarekiko interakzioa murriztea da.

Xehetasunak:

Ahultasun horren bidez, urruneko erasotzaile batek kode arbitrarioa exekuta lezake Fatek Automation-en PLC WinProladder bertsio kaltetuetan. Erabiltzailearen interakzioa behar da ahultasun hori baliatzeko, izan ere, biktimak gune maltzur bat bisitatu edo artxibo maltzur bat ireki beharko luke. Akats espezifikoa PWD artxiboen analisian dago, erabiltzaileak emandako datuen balioztatze egokiaren faltagatik, beraz, osoen gainezkatzea gerta liteke, memorian idatzi aurretik.

Etiketak: 0day, Azpiegitura kritikoak, Ahultasuna

Hainbat ahultasun GE erakundearen UR familiaren produktu batzuetan

Argitalpen data: 2021/03/17

Garantzia: Kritikoa

Kaltetutako baliabideak:

GE erakundeak adierazi du ahultasunek UR familiako honako produktuei eragiten dietela, (B30, B90, C30, C60, C70, C95, D30, D60, F35, F60, G30, G60, L30, L60, L90, M60, N60, T35, T60) babes eta kontrolerako errele aurreratuetan:

- SSH euskarriarekin erlazionatutako ahultasunak: Firmware bertsioak, 7.4x-etik 8.0x-era (CyberSentry aukera);
- Web zerbitzariaren ahultasunak: 8.1x-aren aurreko firmware bertsio guztiak;

- Firmware karga ez boluntarioaren aurkako babesa: 8.1x bertsioaren aurreko oinarrizko segurtasuna duten firmware bertsio guztiak;
- Fabrika modua desaktibatzeko xedapenak: 8.1x bertsioaren aurreko oinarrizko segurtasuna duten firmware bertsio guztiak;
- Last-key pressed erregistrorako sarbidea: 8.1x bertsioaren aurreko oinarrizko segurtasuna duten firmware bertsio guztiak;
- UR abiarazte-kudeatzailearen bitarraren ahultasuna: 7.03/7.04 bertsioen aurreko abiarazte-kudeatzailearen bertsio guztiak.

Azalpena:

SCADA-X, DOEren CyTRICS programa (Energia Saila), Verve Industrial eta VuMetri taldeek 10 ahultasunen berri eman diote GEri: Larritasuna: 1 kritikoa, 5 handiak eta 4 tartekoak.

Konponbidea:

GE erakundeak gomendio hau eman die kaltetutako firmware bertsioak dituzten erabiltzaileei: UR gailuak UR firmwarearen 8.10 bertsiora edo osteko batera eguneratzea, ahultasun horiek konpontzeko. Fabrikatzaileak beste neurri batzuk eta ahultasunen inguruko informazio eman ditu abisu honetan: GES-2021-004.

Xehetasunak:

- UR (Universal Relay) IED (Intelligent Electronic Devices) sistemak, Basic aldagaiarekin, ez du aukerarik ematen Factory Mode desaktibatzeko. Factory erabiltzaile batek IED mantenimendurako erabili ohi du modu hori. Ahultasun kritiko horretarako, CVE-2021-27426 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2016-2183, CVE-2013-2566, CVE-1999-1085, CVE-2021-27422, CVE-2021-27418, CVE-2021-27420, CVE-2021-27428, CVE-2021-27424 eta CVE-2021-27430.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Osasuna, Ahultasuna.

Zerbitzu-ukapena Hitachi ABB Power Grids AFS Series sisteman

Argitalpen data: 2021/03/17

Garrantzia: Ertaina

Kaltetutako baliabideak:

Hitachi ABB Power Grids AFS Series, AFS660/AFS665 ereduak, 7.0.07 bertsioa, honako aldagaiekin:

- AFS660-SR,
- AFS665-SR.

Azalpena:

Hitachi ABB Power Grids taldeak tarteko larritasuneko ahultasun bat antzeman du. Horren bidez, zerbitzu-ukapena gerta liteke AFS seriean, HSR eraztun baten portuetako batean.

Konponbidea:

Hitachi ABB Power Grids taldeak 7.1.03 bertsioa argitaratu du, ahultasun hori konpontzeko, kommutadoreak HSR tramak prozesatzeko modua aldatuz.

Xehetasunak:

Antzemandako ahultasun hori baliatuta, HSR trama manipulatu batek zerbitzu-ukapena eragin lezake HSR eraztun baten portuetako batean. Ahultasun horretarako CVE-2020-9307 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, SCADA, Ahultasuna.

XSS ahultasuna Advantech markako WebAccess/SCADA sisteman

Argitalpen data: 2021/03/17

Garrantzia: Ertaina

Kaltetutako baliabideak:

WebAccess/SCADA, 9.0 bertsioa eta aurrekoak.

Azalpena:

Trend Microren jabetzako TXOne IoT/ICS Security Recearch Labs-eko Chizuru Toyama ikertzaileak tarteko larritasuneko ahultasun baten berri eman dio CISAri. Horren bidez, urruneko erasotzaile batek erabiltzaile baten saioko cookie edo tokenak bahitu litzake, edo webgune maltzur batera bideratu.

Konponbidea:

9.0.1 bertsiora edo osteko batera eguneratzea.

Xehetasunak:

XSS (Cross Site Scripting) ahultasun baten bidez, baimenik gabeko urruneko erasotzaile batek JavaScript kode maltzurra bidal liezaioke erabiltzaile bati, eta, horrela, bere saioko cookie edo tokenak bahituko lituzke, webgune maltzur batera birbideratu, edo nabigatzailean ekintza ez desiratuak burutu. Ahultasun horretarako, CVE-2021-27436 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, SCADA, Ahultasuna.

Hainbat ahultasun Hitachi ABB produktu batzuetan

Argitalpen data: 2021/03/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- eSOMS, 6.0.4.2.2 bertsioaren aurreko 6.0 bertsioak;
- eSOMS, 6.1.4 bertsioaren aurreko 6.1 bertsioak;
- eSOMS, 6.3 bertsioaren aurrekoak;
- eSOMS, Telerik software bertsioa erabiltzen duten 6.3 bertsioaren aurreko guztiak.

Azalpena:

Hitachi ABB Power Grids erakundeak hainbat ahultasunen berri eman dio CISAri. eSOMS produktuetan antzeman dira, eta, horien bidez, erasotzaile batek zerbitzariko irudi bat irakurri eta ezabatu lezake, artxibo-karga arbitrarioak egin, kode arbitrarioa exekutatu, edota babes kriptografikoko mekanismoak apurtu.

Konponbidea:

- eSOMS-era eguneratzea, 6.0.4.2.2, 6.1.4 edo 6.3 bertsioak.
- Informazio gehiago behar izanez gero, harremanetan jarri zentroekin: Hitachi ABB Power Grids contact-centers.

Xehetasunak:

Larritasun kritikoa duten ahultasunak honakoak dira:

- Direktorio mugatu baterako sarbidearen mugatze desegokiaren ondorioz (path traversal), urruneko erasotzaile batek .BMP, .EXIF, .GIF, .ICON, .JPEG, .PNG, .TIFF o .WMF luzapeneko irudi bat irakurri eta ezabatu lezake zerbitzaritik, bereziki diseinatutako eskaera baten bidez. Ahultasun horretarako, CVE-2019-19790 identifikatzailea esleitu da.
- RadAsyncUpload funtzioko .NET deserializazio motako ahultasun bat zifratze-gakoak ezagutzen dituen erasotzaile batek baliatu lezake. Ahultasun horretarako, CVE-2019-18935 identifikatzailea esleitu da.
- Progress Telerik sistemak ez du behar bezala mugatzen erabiltzailearen RadAsyncUpload-erako sarbidea; horrela izanik, urruneko erasotzaileek artxibo-karga arbitrarioak burutu litzakete, edo kode arbitrarioa exekutatu. Ahultasun horretarako, CVE-2017-11357 identifikatzailea esleitu da.
- Telerik.Web.UI sistemak RadAsyncUpload zifratze ahula erabiltzen du. Horrela izanik, urruneko erasotzaileek artxibo-karga arbitrarioak burutu litzakete, edo kode arbitrarioa exekutatu. Ahultasun horretarako, CVE-2017-11317 identifikatzailea esleitu da.
- Telerik.Web.UI.DialogParametersEncryptionKey edo MachineKey sistemen babes desegokiaren ondorioz, urruneko erasotzaileek babes kriptografikoko mekanismoak hautsi litzakete; horrela izanik, MachineKey ihesa, artxibo arbitrarioen karga edo deskarga, XSS ASP.NET ViewState konpromisoa gerta liteke. Ahultasun horretarako, CVE-2017-9248 identifikatzailea esleitu da.

Larritasun handiko gainerako ahultasunei honakoak esleitu zaizkie: CVE-2021-26845, CVE-2014-2217 eta CVE-2014-4958.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Johnson Controls erakundearen exacqVision Web Service sisteman informazioa erakusgai geratu da

Argitalpen data: 2021/03/19

Garrantzia: Ertaina

Kaltetutako baliabideak:

exacqVision Web Service, 20.12.2.0 bertsiora arteko guztiak, hori barne.

Azalpena:

Milan Kyselica ikertzaileak tarteko larritasuneko ahultasun baten berri eman dio Johnson Controls erakundeari. Horren bidez, erasotzaile batek informazio konfidentziala eskura lezake.

Konponbidea:

21.03.3 bertsiora edo osteko batera eguneratzea.

Xehetasunak:

Kaltetutako produktuaren ahultasun baten bidez, urrutiko erasotzaile batek, baimenik gabe, informazio konfidentziala eskura lezake sistema mailan, exacqVision Web Service edo sistema eragileari buruz. Ahultasun horretarako, CVE-2021-27656 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Mugetatik kanpoko idazketa hainbat TRUMPF produktutan

Argitalpen data: 2021/03/23

Garrantziaa: Altua

Kaltetutako baliabideak:

- TruControl, 2.14.0tik 3.14.0rako bertsioak, honako produktuenak:
  - TruPulse,
  - TruDisk,
  - TruDiode,
  - TruFiber,
  - TruMicro2000,
  - TruMicro5000,
  - TruMicro6000,
  - TruMicro7000,
  - TruMicro8000,
  - TruMicro9000,
  - redpowerDirect.

Azalpena:

Qualys Research Labs erakundeak TRUMPF Laser GmbH fabrikatzaileari ahultasun baten berri eman dio: hainbat gailuri eragiten dion idazketatik kanpoko idazketa motakoa da. Fabrikatzaileak erakundeari eman dio ahultasunaren berri.

Konponbidea:

- TruControl 3.16.0 edo osteko bertsioen arabera eguneratzea;
- Bere zerbitzu-bazkidearekin harremanetan jartzea () partxea lortzeko jarraibideak lortzeko.

Xehetasunak:

Heap oinarriko bufferraren gainezkatze motako ahultasun baten bidez (sudon presente dagoena), "sudoedit -s" bidez root-erako pribilegioen eskalatzea burutu liteke, eta kontrabarraren karaktere bakar batekin bukatzen den komandoen-linea argumentu bat. Baimena lortzen duen erasotzaile batek ahultasun hori baliatu lezake, laserraren kontrolean datu-galera eginez, produkzioa geldituz edota laserraren kontrola aldatzearen ondoriozko kalteak eraginez. INCIBE-CERT sisteman argitaratu den ahultasun horretarako CVE-2021-3156 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Moxaren EDR-810 routerretan

Argitalpen data: 2021/03/23

Garrantzia: Altua

Kaltetutako baliabideak:

EDR-810 Series, firmware bertsio hauek:

- 5.7 eta aurrekoak CVE-2014-2284 ahultasunerako;
- 5.1 eta aurrekoak gainerako ahultasunetarako.

Azalpena:

BDU FSTECek 10 ahultasunen berri eman dio Moxari. Horien bidez, urruneko erasotzaile batek zerbitzuaren ukapena eragin lezake, pribilegioetan gora egin, isilpeko informazioa eskuratu eta kode arbitrarioa exekutatu.

Konponbidea:

Firmwarea dagokion bertsiora eguneratzea, fabrikatzailearen laguntza-zerbitzuaren webgunetik.

- 5.8 CVE-2014-2284 ahultasunerako;
- 5.3 gainerako ahultasunetarako.

Xehetasunak:

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Sarrerako balioztatze okerra;
- Zerbitzua ukatzea;
- Pribilegioak handitzea;
- Informazio sentikorra erakusgai jartzea;
- Kodearen urrutiko exekuzioa;
- Zifratze-erroreak;
- man-in-the-middle;
- Sarbide-kontrola, baimenak, pribilegioak;
- Akats numerikoak.

Ahultasun horietarako, honako identifikatzaileak erreserbatu dira: CVE-2014-2284, CVE-2015-1788, CVE-2016-10012, CVE-2015-3195, CVE-2016-6515, CVE-2017-17562, CVE-2013-0169, CVE-2016-0703, CVE-2013-1813 eta CVE-2010-2156.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun GE produktu batzuetan

Argitalpen data: 2021/03/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- MU320E, 04A00.1 bertsioaren aurreko firmware bertsio guztiak;
- Reason DR60, 02A04.1 bertsioaren aurreko firmware bertsio guztiak.

Azalpena:

Tom Westenberg, Thales UK erakundeko ikertzailea eta Thales OT Security Team taldeak 6 ahultasunen berri eman diote GE erakundeari: 2 larritasun kritikokoak, 3 handikoak eta bat baxukoa. Horien bidez, erasotzaile batek pribilegioetan gora egin lezake, gailuaren kontrola eskuratzeko kredentzial kodifikatuak erabili, akatsen erregistradore digitalaren erabateko kontrola hartu (DFR), edota kodea urrunetik exekutatu.

Konponbidea:

Kaltetutako produktuak honako firmware bertsioetara eguneratzea:

- MU320E: 04A00.1 edo ostekoak;
- Reason DR60: 02A04.1 edo ostekoak.

Xehetasunak:

- Kaltetutako softwareak testu argi bidezko pasahitza dauka. Horren bidez, erasotzaile batek fusio-unitatearen kontrola eskuratu lezake, kredentzial hori erabiliz. Ahultasun kritiko horretarako, CVE-2021-27452 identifikatzailea esleitu da.
- Kaltetutako softwareak testu argi bidezko pasahitza dauka, bere sarbide propiorako edo irteera komunikaziorako erabiltzen duena, kanpo osagaiekin. Ahultasun kritiko horretarako, CVE-2021-27440 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2021-27448, CVE-2021-27438, CVE-2021-27454 eta CVE-2021-27450.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Osasuna, Ahultasuna.

Hainbat ahultasun atzeman dira Weintek-en cMT gailuetan

Argitalpen data: 2021/03/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

cMT sistema eragilearen honako modelo eta bertsioak kaltetuta daude:

- cMT-SVR-1xx/2xx, 20210305 bertsioaren aurrekoak;
- cMT-G01/G02, 20210209 bertsioaren aurrekoak;
- cMT-G03/G04, 20210222 bertsioaren aurrekoak;
- cMT3071/cMT3072/cMT3090/cMT3103/cMT3151, 20210218 bertsioaren aurrekoak;
- cMT-HDM, 20210204 bertsioaren aurrekoak;
- cMT-FHD, 20210208 bertsioaren aurrekoak;
- cMT-CTRL01, 20210302 bertsioaren aurrekoak.

Eragina:

Marcin Dudek, CERT.PL zentroko ikertzaileak, 3 ahultasunen berri eman dio CISAri. Denak dira larritasun kritikokoak, eta, horiek baliatuta, baimenik gabeko urruneko erasotzaile batek informazio sentikorra lortu lezake eta kode arbitrarioa exekutatu, root pribilegioak lortzeko.

Konponbidea:

Fabrikatzailearen abisu ofizialeko Solution ataleko eguneratzeak aplikatzea.

Xehetasunak:

- Weintek cMT produktuen linea kodearen injekzioaren mende dago. Horrela izanik, urruneko erasotzaile batek, baimen beharrik gabe, root pribilegioekin exekuta litzake komandoak, kaltetutako sistema eragilean. Ahultasun horretarako, CVE-2021-27446 identifikatzailea esleitu da.
- Weintek produktuen linea sarbide desegokiko hainbat kontrolen eraginpean dago; horrela izanik, erasotzaile batek informazio sentikorra lortu lezake eta administrazio ekintzak burutu, legezko administrari baten izenean. Ahultasun horretarako, CVE-2021-27444 identifikatzailea esleitu da.
- Weintek produktuen linea XSS ahultasun baten mende dago. Horren eraginez, urruneko erasotzaile batek, baimen beharrik gabe, JavaScript kode maltzurra injektatu lezake. Ahultasun horretarako, CVE-2021-27442 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

Hainbat ahultasun Ovarro erakundearen TBox sisteman

Argitalpen data: 2021/03/24

Garrantzia: Altua

Kaltetutako baliabideak:

- TWinSoft, 12.4 bertsioaren aurrekoak eta y 1.46ren aurreko firmware bertsio guztiak;
- TBoxLT2, modelo guztiak;
- TBox MS-CPU32;
- TBox MS-CPU32-S2;
- TBox RM2, modelo guztiak;
- TBox TG2, modelo guztiak.

Azalpena:

Claroty erakundeko Uri Klatz ikertzaileak larritasun handiko bost ahultasunen berri eman du; horien bidez, urruneko erasotzaile batek kodea exekuta lezake, edo zerbitzuaren ukapena eragin.

Konponbidea:

TWinSoft 12.4 bertsiora eta TBoxen firmwarea 1.46 bertsiora egokitzea, fabrikatzailearen webgunearen arreta-gunearen bidez.

Xehetasunak:

- Kodearen sorkuntzan kontrol desegokiaren ahultasuna baliatuz, erasotzaile batek kode maltzurra exekuta lezake, TWinSoft konfigurazioa daukan "ipk" paketeak TBox sisteman kargatu, erauzi eta exekutatu dela kontuan izanda. Ahultasun horretarako, CVE-2021-22646 identifikatzailea esleitu da.
- TBox sistemaren berezko Modbus artxiboetarako sarbiderako funtzioetan baimenen esleipen desegokia egitearen ondorioz, erasotzaile batek konfigurazio-artxiboak irakurri, aldatu edota eliminatu litzake. Ahultasun horretarako, CVE-2021-22648 identifikatzailea esleitu da.
- Erasotzaile batek zerbitzuaren ukapena eragin lezake bereziki diseinatutako Modbus tramak erabiliz, baliabideen kontsumo ez kontrolatuaren motako ahultasuna baliatuz. Ahultasun horretarako, CVE-2021-22642 identifikatzailea esleitu da.
- Erasotzaile batek saio-hasierako pasahitza deszifratu lezake komunikazioen sniffing eta erasoen bidez, kredentzialen babes ez nahikoa aprobetxatuz. Ahultasun horretarako, CVE-2021-22640 identifikatzailea esleitu da.
- TWinSoft-ek 'TwinSoft' erabiltzailerako testuan kodifikatutako zifratze-gakoa erabiltzen du. Ahultasun horretarako, CVE-2021-22644 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.

DLL bahiketa Bosch produktuetan

Argitalpen data: 2021/03/25

Garrantzia: Handia

Kaltetutako baliabideak:

- Bosch BVMS, 9.0.0 bertsioaren aurrekoa;
- Bosch BVMS 10.0.2 bertsioaren aurreko 10.0 bertsioak;
- Bosch BVMS 10.1.1 bertsioaren aurreko 10.1 bertsioak;
- Bosch BVMS Viewer, 9.0.0 bertsioaren aurrekoa;
- Bosch BVMS Viewer, 10.0.2 bertsioaren aurreko 10.0 bertsioak;
- Bosch BVMS Viewer, anteriores a la 10.1.1 bertsioaren aurreko 10.1 bertsioak;
- Bosch Configuration Manager, 7.21.0078 bertsioa edo aurrekoa;
- Bosch DIVAR IP 7000 R2, konfigurazioa: ?using vulnerable BVMS version';
- Bosch DIVAR IP all-in-one 5000, konfigurazioa: ?using vulnerable BVMS version';
- Bosch DIVAR IP all-in-one 7000, konfigurazioa: ?using vulnerable BVMS version';
- Bosch IP Helper, 1.00.0008 bertsioa edo aurrekoa;
- Bosch Monitor Wall, 10.00.0164 bertsioa edo aurrekoa;
- Bosch Video Client, 1.7.6.079 bertsioa edo aurrekoa;

- Bosch Video Recording Manager, 3.71 bertsioa eta aurrekoak;
- Bosch Video Recording Manager, 3.81.0064 bertsioa edo aurreko 3.81 bertsioak;
- Bosch Video Recording Manager, 3.82.0055 bertsioa edo aurreko 3.82 bertsioak;
- Bosch Video Streaming Gateway, 6.45.10 bertsioa edo aurrekoa.

Azalpena:

Boschen hainbat software aplikazio ahultasun baten mende daude. Horren bidez, erasotzaile batek kode gehigarria kargatu lezake DLL gisa; hori aplikazio ahularen abiaraztean exekutatzen da, eta erabiltzailearen testuinguruan

Konponbidea:

- Boschen software aplikazioak bertsio ez ahul batera eguneratzea gomendatzen da.
- Ez badago eguneratzerik eskuragarri, erabiltzaileei arintze-neurri eta konponbide hauekin jarraitzea gomendatzen da:
    - Instalatu gabeko softwarea (esaterako, instalatzaileak eta aplikazio eramangarriak eurak) ez da beste erabiltzaile batzuek sarbide duten direktorioetatik exekutatu behar, edo maltzurrak izan litezkeen DLLak dauden direktorioetatik (esaterako, "deskargen" berezko direktorioa).
    - Ez dago software mota horretarako ibilbide segururik, beraz, eragin potentziala instalatzaile bat edo aplikazio eramangarri bat kargatzen diren direktorioaren araberakoa da ("AppDir"):
    -
        - Berezko "deskarga" direktorioa: Bitar maltzurrak erabiltzaile baten berezko deskarga karpetan egon litezke, horren aurretiko interakzioa dela eta (esaterako, deskarga-lotura maltzur batean klik eginez, drive-by-download bat exekutatzea lortzen duen leku bat bisitatuz), eta exekutagarri batek karga litzake. Arintze neurri moduan, erabiltzaileei gomendatzen zaie exekutagarriak deskarga direktorioetatik beste direktorio batzuetara mugitzea, beste erabiltzaile batzuek sarbiderik ez dutena, eta bertatik soilik hastea exekutagarriak. Orokorrean, berezko deskarga direktoriotik zuzenean instalazioak edota aplikazioak exekutatzea ez da gomendagarria, ezta nabigatzaile batean eskatutako deskarga-eskaerak ere.Pribilegio gutxiko erabiltzaile batzuek sarbidea duten direktorio batzuk: Direktorio hori ez du softwareak berak sortu (esaterako, aldi baterako direktorio bat instalazio-denboran), babestu gabeko instalazio direktorio bat da, beraz, sistema ahularen konfigurazioarena. Pribilegio gutxiko erabiltzaileek idazketa baimenak dituzten direktorioetan exekutagarriak ez jartzeko gomendioa egiten da, bereziki. Kontuan izan erabiltzaileak C: eremuan sortutako direktorioek (esaterako, C: /NireKarpetaBerria) beste erabiltzaile batzuentzako idazketa baimenak jasoko lituzketela oinordetzan, beraz, ez da batere gomendagarria.

Xehetasuna:

- Kontrolatu gabeko bilaketa-ibilbide baten bidez DLL bat kargatzearen ondorioz, erasotzaile batek kode arbitrarioa exekuta lezake biktimaren sisteman. Horretarako, biktima engainatu behar da IP Helper aplikazio eramangarriaren aplikazio-direktorio berean DLL maltzur bat kokatzeko. Ahultasun horretarako, CVE-2020-6771 identifikatzailea esleitu da.
- Kontrolatu gabeko bilaketa-ibilbide baten bidez DLL bat kargatzearen ondorioz, erasotzaile batek kode arbitrarioa exekuta lezake biktimaren sisteman. Horrek instalatzaileari zein instalatutako aplikazioari eragiten die. Ahultasun horretarako, CVE-2020-6785 identifikatzailea esleitu da.
- Kontrolatu gabeko bilaketa-ibilbide baten bidez DLL bat kargatzearen ondorioz, erasotzaile batek kode arbitrarioa exekuta lezake biktimaren sisteman. Horretarako, biktima engainatu egin behar da instalatzailea hasten den direktorio berean DLL maltzur bat kokatzeko. Ahultasun horietarako CVE-2020-6786, CVE-2020-6787, CVE-2020-6788 eta CVE-2020-6789 identifikatzaileak esleitu dira.
- Kontrolatu gabeko bilaketa-ibilbide baten bidez exekutagarri bati deitzearen ondorioz, erasotzaile batek kode arbitrarioa exekuta lezake biktimaren sisteman. Horretarako, biktima engainatu egin behar da instalatzailea hasten den direktorio berean .exe maltzur bat kokatzeko. Ahultasun horretarako, CVE-2020-6790 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Azpiegitura kritikoak, Ahultasuna.