2020ko urtarrilaren Bulletina

Ohartarazpenak - Kontrol Industrialeko Sistemak

Ahultasuna WECONen PIStudio-n

Argitalpen data: 2020/01/02

Garrantzia: Altua

Kaltetutako baliabideak:

- PIStudio, bertsio guztiak.

Azalpena:

Trend Micro Zero Day Initiative-ko Mat Powell-ek PIStudio-k duen ahultasun baten berri eman du. Hori baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

Oraingoz ez dago konponbiderik eskuragarri.

Xehetasuna:

Erabiltzaileak sartutako datuen baliozkotze falta baliatuz, erasotzaile batek esleitutako objektuaren amaieratik harago idatz lezake, administratzaile pribilegioekin urruneko kodea exekutatzeko.

Etiketak: 0day

Ahultasuna Moxa-ren MGate 5105-MB-EIP Series-en

Argitalpen data: 2020/01/07

Garrantzia: Altua

Kaltetutako baliabideak:

- MGate 5105-MB-EIP Series, firmware-aren 4.1 eta lehenagoko bertsioak.

Azalpena:

MGate 5105-MB-EIP Series-ek duen ahultasun baten berri eman da. Hori baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

Firmware/softwarearen bertsio berrira eguneratzea.

Xehetasuna:

.MGate 5105-MB-EIP Series-en web zerbitzariak duen komandoen injekzio erako ahultasun bat baliatuz erasotzaile batek urruneko kodea exekuta lezake. Ahultasun horretarako ez da identifikatzailerik esleitu.

Etiketak: Eguneraketa, Ahultasuna

Lehenetsitako SSH gakoen erabilpena Meinberg-en SyncBox-en

Argitalpen data: 2020/01/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

SyncBox/PTP eta SyncBox/PTPv2ren bertsio guztiak, erabiltzaileak berak eskuz host SSHren inolako gakorik ordezkatu ez badu.

Azalpena:

Simon Winter ikertzaileak SyncBox gailuei eragiten ahultasun baten berri eman du. Ahultasun hori arrakastaz baliatuz gero urruneko erasotzaile batek man-in-the-middle erako erasoak egin litzake modu errazagoan eta gailuaren kredentzialak eskuratu.

Konponbidea:

Meinberg-ek gomendatzen du gailuetan erabilitako SSH gakoak ordezkatzea bere *firmware*-a eguneratzeko garatutako tresna erabiliz.

Xehetasuna:

SyncBox gailuek lehenetsitako SSH gakoak erabiltzen dituzte. Horrek eragiten du MitM (*man-in-the-middle*) erako erasoak emankorragoak izatea, administratzaile sarbidearen kredentzialak eskuratu nahi direnean sarearen bitartez *passphrase*-aren kontsulta bat egin gabe. Ahultasun horretarako CVE-2019-17584 identifikatzailea erreserbatu da.

Etiketak: Komunikazioak, Ahultasuna

Hainbat ahultasun Siemens gailuetan

Argitalpen data: 2020/01/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SCALANCE X-200 switchen familia (SIPLUS NETen aldaera guztiak barne), v5.2.3 bertsioa baino lehenagoko guztiak;
- SCALANCE X-200 IRT switchen familia (SIPLUS NETen aldaera guztiak barne), v5.4.1 bertsioa baino lehenagoko guztiak;
- SCALANCE X-200RNA switchen familia;
- SCALANCE X300 switchen familia (SIPLUS NETen aldaera guztiak barne), v4.1.3 bertsioa baino lehenagoko guztiak;
- SCALANCE X408, v4.1.3 bertsioa baino lehenagoko guztiak.
- SINEMA zerbitzaria, V14.0 SP2 baino lehenagoko bertsio guztiak.
- TIA Portal:
  - V14, bertsio guztiak;
  - V15, V15.1 Upd 4 baino lehenagoko bertsio guztiak;
  - V16, bertsio guztiak;
- SINAMICS PERFECT HARMONY GH180 drives:
  - MLFB 6SR32...-. . . ..-. . . ;
  - MLFB 6SR4. . . -. . . ..-. . . ;
  - MLFB 6SR5. . . -. . . ..-. . . ., A30 aukerarekin (12 hazbeteko HMI)
  - MLFB 6SR325.-. . . ..-. . . . (Eskuragarritasun altua);

Azalpena:

Hainbat ikertzailek gailuei eragiten dieten sei ahultasunen berri eman diote Siemensi, hiru larritasun ertainekoak, bi altukoak eta bat kritikoa. Urruneko erasotzaile batek kode arbitrarioa exekuta lezake, sarbide murrizpenak saihestu, pribilegioak eskalatu eta konfigurazioak aldatu. Horrela konfidentzialtasunari, integritateari eta eskuragarritasunari eragingo litzaieke.

Konponbidea:

Ahultasunak konpontzeko, Siemensek gomendatzen du kaltetutako gailuak ondoko bertsio hauetara eguneratzea:

- SCALANCE X-200: v5.2.3 bertsiora eguneratzea.
- SCALANCE X-200 IRT: v5.4.1 bertsiora eguneratzea;
- SCALANCE X-300 eta X408: v4.1.3 bertsiora eguneratzea;
- SINEMA zerbitzaria: V14.0 SP2 Update1 bertsiora eguneratzea;
- SCALANCE X-200RNA:
  - ACLak konfiguratzea webean oinarritutako mantenua IP fidagarriei soilik baimentzeko;
  - Webean oinarritutako mantenua (WBM) desgaitzea eta gailua konfiguratzeko SSH erabiltzea.
- SINAMICS PERFECT HARMONY GH180 drives-en kasuan Siemensek gomendatzen du laguntza zerbitzuarekin harremanetan jartzea behar diren konfigurazioak eskuratzeko.
- ActiveX-en erabilerari dagokionez, Siemensek gomendatzen du fabrikatzaile honen berezko baliabideetara soilik sarbidea izatea, hirugarren parteen kontrolatu gabeko softwarea exekutatzea saihesteko. Gainera, fabrikatzaileak gomendatzen du praktika onen gidak jarraitzea, bai bere softwarearen instalazioan eta bai sistema guztiak gotortzeko moduan.

Xehetasuna:

Ondoren zehazten dira ahultasun kritikoak:

- Saioen baliozkotze oker bat baliatuz urruneko erasotzaile batek, sisteman baliagarria den baina pribilegio gutxi dituen saio batekin, firmwarearen eguneraketak eta beste eragiketa administratibo batzuk egin litzake konektatutako gailuetan. Ahultasun horretarako CVE-2019-10940 identifikatzailea erreserbatu da.

Kritikotasun altuko ahultasunak:

- Urruneko erasotzaile batek informazio sentikorra eskura lezake edo gailuaren konfigurazioak aldatu. Ahultasun horretarako CVE-2019-13933 identifikatzailea erreserbatu da.
- Konfigurazio fitxategien edukian egindako aldaketa batzuk baliatuz, erasotzaile batek kode arbitrarioa exekuta lezake SYSTEM

pribilegioekin. Ahultasun horretarako CVE-2019-10934 identifikatzailea erreserbatu da.

Kritikotasun ertaineko ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2019-19278, CVE-2018-4848 eta CVE-2018-4842.

Etiketak: Eguenraketa, Siemens, Ahultasuna

Hainbat ahultasun OSIsoft-en PI Vision-en

Argitalpen data: 2020/01/15

Garrantzia: Altua

Kalatetutako baliabideak:

- 2019. urtea baino lehenagoko PI Vision-en bertsio guztiak;
- PI Vision 2017 R2 eta R2 SP1.

Azalpena:

OSIsoft-ek 4 ahultasunen berri eman du, bat kritikotasun altukoa eta hiru ertainekoak. Urruneko erasotzaile batek informazio sentikorra ezagutzera eman lezake edo gailuaren eskuragarritasuna mugatu.

Konponbidea:

Ahultasun horiek konpontzeko OSIsoft-ek gomendatzen du PI Vision 2019ren azken bertsiora eguneratzea.

Xehetasuna:

- Kritikotasun altuko ahultasuna Cross-site Request Forgery erakoa da eta PI Vision-en administrazio webaren orrialdean sartua izan liteke. Ahultasun horretarako CVE-2019-18271 identifikatzailea erreserbatu da.
- Larritasun ertaineko gainerako ahultasunetarako CVE-2019-18275, CVE-2019-18273 eta CVE-2019-18244 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Ahultasuna

Sarrera datuen baliozkotze okerra GE/Emerson-en PACSystems RX3i-n

Argitalpen data: 2020/01/15

Garrantzia: Altua

Kaltetutako baliabideak:

- CPE100, R9.85 bertsioaren aurreko guztiak;
- CPE115, R9.85 bertsioaren aurreko guztiak;
- CPE302, R9.90 bertsioaren aurreko guztiak;
- CPE305, R9.90 bertsioaren aurreko guztiak;
- CPE310, R9.90 bertsioaren aurreko guztiak;
- CRU320, katalogotik ateratako produktua da, CPE330rekin ordezkatzekoa;
- CPE330, R9.90 bertsioaren aurreko guztiak;
- CPE400, R9.90 bertsioaren aurreko guztiak;
- CPL410, R9.90 bertsioaren aurreko guztiak.

Azalpena:

Yeop Chang ikertzaileak kritikotasun altuko ahultasun baten berri eman du, GE/Emerson-en gailuei eragiten diena. Urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake gailuan.

Konponbidea:

Emerson-ek honako bertsio hauetara eguneratzea gomendatzen du:

- R9.85 bertsioa:
  - CPE100;
  - CPE115;
- R9.90 bertsioa:
  - CPE302;
  - CPE305;
  - CPE310;
  - CPE330;
  - CPE400;
  - CPE410;

CPU/CRU320ren kasuan Emerson-ek jakinarazi du bere bizitza zikloaren amaierara iritsi dela eta CPE330rekin ordeztea gomendatzen du.

Xehetasuna:

Bereziki diseinatutako paketeak bidaliz modulua geldialdi egoerara aldatzea eragin liteke, eta ondorioz zerbitzuaren ukapen egoera sortu. Urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake. Ahultasun horretarako CVE-2019-13524 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna Windows-en CryptoAPI-n

Argitalpen data: 2020/01/21

Garrantzia: Altua

Kaltetutako baliabideak:

Microsoft Windows 10 IoT Core eta Enterprise duten bertsioak kaltetuta daude.

- Rockwell Automation:
  - CompactLogix 5480 Controllers;
  - FactoryTalk Analytics for Devices;
  - FactoryTalk Analytics LogixAI;
  - ControlLogix Compute Module (1756-CMS1B1).

Azalpena:

Microsoft ha reportado una vulnerabilidad de criticidad alta que podría afectar a productos de varios fabricantes. Un atacante remoto podría falsear un certificado y firmar ejecutables maliciosos.

Konponbidea:

Microsoftek segurtasuneko eguneraketa automatiko bat argitaratu du ahultasun hori konpontzeko.

- Rockwell Automation:
  - FactoryTalk Analytics for Devices eta FactoryTalk Analytics LogixAI gailuek ahultasuna konponduko duen firmwarearen eguneraketa bat beharko dute. Eguneraketa hori Rockwell Automation-ek argitaratuko du.
  - Kaltetutako gainerako gailuek Microsoftek eskainitako segurtasun eguneraketa aplika dezakete.

Xehetasuna:

Microsoftek kritikotasun altuko ahultasun baten berri eman du, hainbat fabrikatzaileren produktuei eragin liezaiekeena. Urruneko erasotzaile batek ziurtagiri bat faltsutu lezake eta asmo gaiztoko exekutagarriak sinatu.

Etiketak: Eguneraketa, Microsoft, Ahultasuna, Windows

Hainbat ahultasun Honeywell-en produktuetan

Argitalpen data: 2020/01/22

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- MAXPRO VMS:
  - HNMSWVMS, VMS560 Build 595 T2-Patch bertsioa baino lehenagokoa;
  - HNMSWVMSLT, VMS560 Build 595 T2-Patch bertsioa baino lehenagokoa;
- MAXPRO NVR:
  - MAXPRO NVR XE, NVR 5.6 Build 595 T2-Patch bertsioa baino lehenagokoa;
  - MAXPRO NVR SE, NVR 5.6 Build 595 T2-Patch bertsioa baino lehenagokoa;
  - MAXPRO NVR PE, NVR 5.6 Build 595 T2-Patch bertsioa baino lehenagokoa;
  - MPNVRSWXX, NVR 5.6 Build 595 T2-Patch bertsioa baino lehenagokoa.

Azalpena:

Joachim Kerschbaumer-ek larritasun kritikoak dituzten bi ahultasunen berri eman du, Honeywell-en ekipoei eragiten dietenak. Urruneko erasotzaile batek pribilegioen eskalatzea egin lezake, zerbitzuaren ukapen egoera eragin edo kodearen exekuzioa ahalbidetu.

Konponbidea:

Honeywell-ek ahultasunak konpontzen dituzten bi eguneraketa argitaratu ditu:

- VMS 560 Build 595 T2-Patch, VMS sistemetarako;
- NVR 5.6 Build 595 T2-Patch, NVR sistemetarako.

Eguneraketa horiek Honeywell-en MyWebTech zerbitzu orrialdean aurki daitezke, soilik erabiltzaile erregistratuentzat.

Xehetasuna:

- Produktuak ahulak dira fidagarriak ez diren datuen deserializazio baten aurrean. Autentifikaziorik gabeko urruneko erasotzaile batek datu horiek alda litzake bereziki diseinatutako web eskarien bitartez, eta horrek kodea exekutatzera ere eraman lezake. Ahultasun horretarako CVE-2020-6959 identifikatzailea erreserbatu da.
- Beste ahultasuna SQL injekzio bat da. Autentifikaziorik gabeko urruneko erasotzaile batek web interfazera sarbidea lor lezake administratzaile baimenekin. Ahultasun horretarako CVE-2020-6960 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun General Electric-en produktuetan

Argitalpen data: 2020/01/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

GE Healthcare Monitoring plataformen ondoko bertsioak kaltetuta daude:

- B850, versión 2.X (Afectado por CVE-2020- 6962 y CVE-2020-6965).ApexPro Telemetry Server, 4.2 eta lehenagoko bertsioak;
- CARESCAPE Telemetry Server, 4.2 eta lehenagoko bertsioak;
- Clinical Information Center (CIC), 4.X eta 5.X bertsioak;
- CARESCAPE Telemetry Server, 4.3 bertsioa (CVE-2020- 6962 eta CVE-2020-6961ek eraginda);
- CARESCAPE Central Station (CSCS), 1.X bertsioak;
- CARESCAPE Central Station (CSCS), 2.X bertsioak (CVE-2020-6962 eta CVE-2020-6964-k eraginda);
- B450, 2.X bertsioa (CVE-2020-6962 eta CVE-2020-6965ek eraginda);
- B650, 1.X bertsioa (CVE-2020-6962 eta CVE-2020-6965ek eraginda);
- B650, 2.X bertsioa (CVE-2020-6962 eta CVE-2020-6965ek eraginda);
- B850, 1.X bertsioa (CVE-2020-6962 eta CVE-2020-6965ek eraginda);
- B850, 2.X bertsioa (CVE-2020-6962 eta CVE-2020-6965ek eraginda).

Azalpena:

CyberMDXeko Elad Luz-ek GEren produktuei eragiten dieten era ezberdinetako ahultasunen berri eman du: kredentzialen biltegiratze ez-babestua, sarreraren egiaztapen desegokia, kredentzialen erabilpena kodean, funtzio kritikoetarako autentifikazio falta, arriskutsuak izan litezkeen fitxategien igoera ez-murriztua eta zifratzearen sendotasun desegokia. Ahultasun horiek arrakastaz baliatuz gero, erasotzaile batek hainbat saretara sarbidea lor lezake, gailuen monitorizazioa gal dadin eragin, sistema eragilean aldaketak egin eta kode arbitrarioa exekutatu.

Konponbidea:

Fabrikatzaileak erabiltzaileei gomendatzen die MC eta IX sareak ondo konfiguratuta daudela baieztatzea, isolamenduak eta konfigurazioak Patient Monitoring Network Configuration Guide, CARESCAPE Network Configuration Guide-n eta produktuaren eskuliburu teknikoetan eta zerbitzuari buruzkoetan zerrendatzen diren baldintzak betetzen dituztela bermatzeko. Horiek eskuratzeko GErekin harremanetan jarri beharra dago bezeroaren laguntzarako atariaren bidez zerbitzua jasotzeko baliagarria den kontu batekin.

Horrez gain, GE software eguneraketak/partxeak garatzen ari da segurtasun hobekuntza osagarriekin. Erabiltzaileak GEren segurtasun webgunean sar daitezke informazio eguneratuagoa eskuratzeko.

Xehetasuna:

- Kaltetutako produktuetan dagoen ahultasuna baliatuz, erasotzaile batek konfigurazio fitxategitako SSH gako pribatura sarbidea lor lezake. Ahultasun horretarako CVE-2020-6961 identifikatzailea erreserbatu da.
- Webean oinarritutako sistemaren konfigurazio utilitateak duen sarreraren egiaztatze erako ahultasun bat baliatuz, erasotzaile batek urruneko kode arbitrarioaren exekuzioa egin lezake. Ahultasun horretarako CVE-2020-6962 identifikatzailea erreserbatu da.
- Kaltetutako produktuek kodean barneratutako SMB kredentzialak erabili zituzten, eta hori baliatuz erasotzaile batek kode arbitrarioa exekuta lezake urrunetik. Ahultasun horretarako CVE-2020-6963 identifikatzailea erreserbatu da.
- Kaltetutako gailuetako teklatuaren kommutazio zerbitzu integratua baliatuz, erasotzaileek teklatuaren sarrerara urruneko sarbidea lor lezakete sare bitartez autentifikatu behar izan gabe. Ahultasun horretarako CVE-2020-6964 identifikatzailea erreserbatu da.
- Softwarea eguneratzeko mekanismoak duen ahultasun bat baliatuz, autentifikatutako erasotzaile batek sisteman fitxategi arbitrarioak karga litzake, prestatutako eguneraketa pakete baten bidez. Ahultasun horretarako CVE-2020-6965 identifikatzailea erreserbatu da.
- Kaltetutako produktuek zifratze eskema ahul bat erabiltzen dute mahaigainen urruneko kontrolerako, eta hori baliatuz erasotzaile batek kodearen urruneko exekuzioa egin lezake sareko gailuetan. Ahultasun horretarako CVE-2020-6966 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Osasuna, Ahultasuna

Zerbitzuaren ukapena CODESYSen hainbat produktutan

Argitalpen data: 2020/01/24

Garrantzia: Altua

Kaltetutako baliabideak:

- BeagleBone-rako CODESYS Control, V3.5.15.30 baino lehenagoko bertsioak;
- emPC-A/iMX6-erako CODESYS Control, V3.5.15.30 baino lehenagoko bertsioak;
- IOT2000rako CODESYS Control, V3.5.15.30 baino lehenagoko bertsioak;
- Linuxerako CODESYS Control, V3.5.15.30 baino lehenagoko bertsioak;
- PLCnext-erako CODESYS Control, V3.5.15.30 baino lehenagoko bertsioak;
- PFC100erako CODESYS Control, V3.5.15.30 baino lehenagoko bertsioak;
- PFC200rako CODESYS Control, V3.5.15.30 baino lehenagoko bertsioak;
- Raspberry Pi-rako CODESYS Control, V3.5.15.30 baino lehenagoko bertsioak;
- RTE V3-rako CODESYS Control, V3.5.15.30 baino lehenagoko bertsioak;
- CODESYS Control RTE V3 (Beckhoff CXerako), V3.5.15.30 baino lehenagoko bertsioak;
- CODESYS Control Win V3, V3.5.15.30 baino lehenagoko bertsioak;
- CODESYS Control V3 Runtime System Toolkit, V3.5.15.30 baino lehenagoko bertsioak;
- CODESYS V3 Safety SIL2, V3.5.15.30 baino lehenagoko bertsioak;
- CODESYS Gateway V3, V3.5.15.30 baino lehenagoko bertsioak;
- CODESYS HMI V3, V3.5.15.30 baino lehenagoko bertsioak;
- CODESYS V3 Simulation Runtime, V3.5.15.30 baino lehenagoko bertsioak.

Azalpena:

3S-Smart Software Solutions GmbH-k kritikotasun altuko ahultasun baten berri eman du, CODESYS gailuei eragiten diena. Urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake.

Konponbidea:

Ahultasuna konpontzeko 3S-Smart Software Solutions GmbH-k aholkatzen du bere gailuak 3.5.15.30 bertsiora eguneratzea. Bere deskarga zentroan eskura daiteke.

Xehetasuna:

CODESYS gailuak kaltetuta gera litezke erasotzaile batek beroietara eskaera aldatuak bidaliko balitu. Horrela kontrolatu gabeko memoriaren esleipena eragingo luke eta gailuetan zerbitzuaren ukapen egoera gerta liteke. Ahultasun horretarako CVE-2020-7052 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Schneider Electric-en Operator Terminal Expert-en

Argitalpen data: 2020/01/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

EcoStruxure Operator Terminal Expert.

Azalpena:

Schneider Electric-ek adierazi duenez, EcoStruxure Operator Terminal Expert produktuak DLL arbitrarioaren karga erako eta bideetarako sarbide ez-kontrolatu erako bi ahultasun ditu, Pwn2Own ekitaldian aurkituak.

Konponbidea:

Oraingoz ez dago ahultasun horiek konpontzen dituen eguneraketarik. Schneider Electric fabrikatzaileak horretan dihardu lanean, ahalik eta azkarren argitaratzearren.

Eguneraketa hori argitaratzen duen bitartean, fabrikatzaileak ondoko neurri prebentiboak hartzea gomendatzen du:

- Lan estazioak babestea zibersegurtasun arloko praktika onenak jarraituz (antibirusa, sistema eragile eguneratuak, pasahitz seguruen politika, aplikazioen zerrenda zuriko softwarea, eta abar), Schneider Electric-en Praktikarik onenak gidan azaldutakoak.
- EcoStruxure Operator Terminal Expert softwarea ez exekutatzea Windows-eko administratzaile pribilegioekin.
- Lan estazioa suebaki batekin babestea eta sare fidagarri batean erabiltzen dela ziurtatzea.
- HMI produktua sare seguru batean instalatzea.
- EcoStruxure Operator Terminal Expert softwarea lan estazio seguru batean soilik erabiltzea.
- Proiektu fitxategiak soilik fidagarriak diren erabiltzaileengandik onartzea.
- HMIra aplikazio fidagarriak soilik simulatzea / transferitzea.
- Proiektuko fitxategiak eta esportatutako fitxategiak modu seguruan administratzea, informazioaren hedapena edo datuen ustekabeko aldaketak saihestearren.
- Zure proiektuan pasahitz segurua ezartzea. Proiektuen babesa hobetzearren, "Pasahitz konplexua erabili" aukera gaitzea "Segurtasuna / Konfigurazioa / Pasahitz konplexua erabili" atalean.

Xehetasuna:

Pwn2Own ekitaldian segurtasun ikertzaileek EcoStruxure Operator Terminal Expert produktuak dituen DLL arbitrarioaren karga erako eta direktorioaren jauzi erako ahultasunen berri eman zuten. Ahultasun horietarako identifikatzailerik ez da erreserbatu oraindik.

Etiketak: 0day, Schneider Electric, Ahultasuna

EKANS ransomwareak GEren Proficy produktuen bertsio guztiei eragiten die

Argitalpen data: 2020/01/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

GE Proficy softwarearen lizentziadun bertsio guztiak.

Azalpena:

GE fabrikatzaileak antzeman duenez, EKANS ransomwarearen xede diren prozesuen zerrendan Proficy produktuen erreferentzia asko jasotzen dira, bai eta fabrikatzaile horren lizentzien zerbitzu bat ere. Kutsatze hori EKANS ransomwareak sortua izan liteke. Malware mota hau erabiltzen duten erasotzaileek diskoa zifratu lezakete eta zerbitzuaren ukapen egoera sortu, *kill* seinaleak bidaliz exekuzioan dauden prozesuetan.

Konponbidea:

Fabrikatzaileak bere bezeroei aholkatzen die egiaztatzea euren antibirus hornitzailea gai dela EKANS ransomwarea detektatzeko. Horrez gain, Praktika onen gida 7.0 jarraitzea aholkatzen die bere produktuak, horien artean Proficy softwarea, hedatu eta inplementatzerakoan.

Xehetasuna:

EKANS ransomwareak eragiten dituen aktiboen disko gogorra zifratzeko eta segurtasun kopiak ezabatzeko zifratze estandarreko funtzioak erabiltzen ditu WMI (*Windows Management Interface*) bidez. Zifratze eragiketa horien aurretik malware honek GE produktuekin zerikusia duten prozesu asko gelditzen ditu *kill* seinaleak bidaltzeari esker, eta haren lizentzien zerbitzua ere bai. Fabrikatzailearen informazioaren arabera, ransomware honek ez du hedatze mekanismorik eta nahitaez erabiltzaile batek abiarazi beharra du modu interaktiboan, edo bestela *host*-a kutsatzen duen *script* bat exekutatuz.

Etiketak: Malwarea, Ahultasuna

Hainbat ahultasun Bosch-en produktuetan

Argitalpen data: 2020/01/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Bosch BVMS Viewer, honako bertsioak:
  - 7.5 baino lehenagokoak, bera barne;
  - 10.0.0.1225 baino lehenagokoak, bera barne, konfigurazio honekin: patch for security issue 211404, 241463 not installed;
- Bosch Video Management System, honako bertsioak:
  - 7.5 baino lehenagokoak, bera barne;
  - 10.0.0.1225 baino lehenagokoak, bera barne, konfigurazio honekin: patch for security issue 211404, 241463 not installed;
- Bosch DIVAR IP, modelo hauek:
  - 7000, konfigurazio hauekin: vulnerable BVMS version installed edo vulnerable BVMS MVS version installed;
  - all-in-one 5000, konfigurazio hauekin: vulnerable BVMS version installed edo vulnerable VSG version installed;
  - 5000, 3.80.0039 bertsioa baino lehenagokoak, bera barne, konfigurazio honekin: port 8023 on device's firewall opened explicitly and vulnerable VSG version installed;
  - 3000, konfigurazio hauekin: vulnerable VSG version installed edo vulnerable BVMS MVS version installed;
  - 2000, 3.62.0019 bertsioa baino lehenagokoak, bera barne, konfigurazio honekin: port 8023 on device's firewall opened explicitly and vulnerable VSG version installed;
- Bosch Video Streaming Gateway, honako bertsioak:
  - 6.42 eta lehenagokoak, 6.42.10 bitartean, bera barne;
  - 6.43tik 6.43.0023 bitartean, bera barne;
  - 6.44tik 6.44.0030 bitartean, bera barne;
  - 6.45etik 6.45.08 bitartean, bera barne;
- Bosch BVMS Mobile Video Service, honako bertsioak:
  - 7.5 baino lehenagokoak, bera barne;
  - 8.0.0.329 baino lehenagokoak, bera barne, konfigurazio honekin: patch for security issue 243748 not installed;
  - 9.0.0.827 baino lehenagokoak, bera barne, konfigurazio honekin: patch for security issue 243748 not installed;
  - 10.0.0.1225 baino lehenagokoak, bera barne, konfigurazio honekin: patch for security issue 243748 not installed.

Azalpena:

Bosch-en hainbat gailuri eragiten dieten 4 ahultasunen berri eman da, 2 kritikoak eta 2 altuak. Ahultasun horiek arrakastaz baliatuz gero, urruneko erasotzaile batek kodearen exekuzio erako erasoak ausaz egin litzake, VSG konfigurazioa aldatu, informaziora sarbidea lortu eta gailuetatik fitxategi sentikorrak eskuratu.

Konponbidea:

Bosch-ek gomendatzen du kaltetutako gailuak ahultasun horiek eragiten ez duten bertsio eguneratu batera eguneratzea, ohar bakoitzaren Affected Hardware eta Affected Software ataletan zehazten direnak.

Xehetasuna:

- Autentifikatu gabeko urruneko erasotzaile batek kontrolatu gabeko bideetarako sarbide erako (path traversal) ahultasuna balia lezake, eta BVMS (Bosch Video Management System) zerbitzuari eragin. Ahultasun horretarako CVE-2020-6768 eta CVE-2020-6767 identifikatzaileak erreserbatu dira.
- Urruneko erasotzaile batek sare interfazearen bidez autentifikazioaren gabezia erako ahultasun bat balia lezake BVSG (Bosch Video Streaming Gateway) gailuetara sartzeko eta konfigurazio datu arbitrarioak berreskuratzeko edo aldatzeko. Ahultasun horretarako CVE-2020-6769 identifikatzailea erreserbatu da.
- Urruneko erasotzaile batek, sare interfazearen bidez, fidagarriak ez diren datuen deserializazio erako ahultasun bat balia lezake kode arbitrarioa exekutatzeko. Ahultasun horretarako CVE-2020-6770 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna