2019ko Irailaren Bulletina

Ohartarazpenak - Teknikoak

Partekatutako direktorioa saihestea Samba-n

Argitalpen data: 2019/09/04

Garrantzia: Altua

Kaltetutako baliabideak:

- Samba, 4.9.0 bertsiotik 4.9.12 bertsiora bitartekoak;
- Samba, 4.10.0 bertsiotik 4.10.7 bertsiora bitartekoak.

Azalpena:

SerNet-eko Stefan Metzmacher segurtasun ikertzaileak, Samba-ko ekipoarekin lankidetzan, kritikotasun altuko ahultasun bat aurkitu du. Autentifikatutako erasotzaile batek direktorioa saihets lezake partekatutako direktoriotik kanpo.

Konponbidea:

- Samba 4.9.X: partxea aplikatzea edo 4.9.12 bertsiora eguneratzea;
- Samba 4.10.X: partxea aplikatzea edo 4.10.7 bertsiora eguneratzea.

Sambaren lehenagoko bertsioetarako, eguneraketak argitaratuz joango dira Samba-ren deskargen zentroan.

Sambaren administratzaileei aholkatzen zaie bertsio horietara eguneratzea edo partxea lehenbailehen aplikatzea.

Xehetasuna:

Ahultasunaren jatorria smb.conf konfigurazio fitxategiko zenbait parametro dira. Autentifikatutako erasotzaile batek direktorioa saihets lezake partekatutako direktoriotik kanpo. Ahultasun horretarako CVE-2019-10197 identifikatzailea erabili da.

Etiketak: Eguneraketa, Samba, Ahultasuna

Kodearen urruneko exekuzio erako hainbat ahultasun Aruba Mobility Controllers-en

Argitalpen data: 2019/09/04

Garrantzia: Altua

Kaltetutako baliabideak:

Aruba Mobility Controllers, firmwarearen ondoko bertsioak dituztenak:

- ArubaOS 6.x, 6.4.4.21 baino lehenagoko bertsioa;
- ArubaOS 6.5.x, 6.5.4.13 baino lehenagoko bertsioa;
- ArubaOS 8.x, 8.2.2.6 baino lehenagoko bertsioa;
- ArubaOS 8.3.0.x, 8.3.0.7 baino lehenagoko bertsioa;
- ArubaOS 8.4.0.x, 8.4.0.3 baino lehenagoko bertsioa.

Azalpena:

Aruba-k jakinarazi du Aruba Mobility Controllers-en exekutatzen diren bertsio batzuek ahultasunak dituztela. Horiek baliatuz, erasotzaile batek kode arbitrarioa exekuta lezake azpiko sistema eragileak sistemaren pribilegio guztiekin.

Konponbidea:

Ondoko eguneraketak aplikatzea, kaltetutako bertsioaren arabera:

- ArubaOS 6.4.4.21,
- ArubaOS 6.5.4.13,
- ArubaOS 8.2.2.6,
- ArubaOS 8.3.0.7,
- ArubaOS 8.4.0.3,
- ArubaOS 8.5.0.0.

Xehetasuna:

- *Network-listener* osagaiak kodearen urruneko exekuzio erako ahultasuna dauka ArubaOSren bertsio batzuetan. Erasotzaile batek, mugikortasun kontrolatzaile bati bereziki diseinatutako IP trafikoa transferitzeko gaitasuna balu, PAPI protokoloa (UDP 8211) baliatuz, prozesuan akats bat eragin lezake, edo azpiko sistema eragilean kode arbitrarioa exekutatu sistemaren pribilegio guztiekin. Ahultasun horretarako CVE-2018-7081 identifikatzailea erreserbatu da.
- ArubaOS softwarearen web osagai batzuk ahulak dira CRLF injekzioaren eta islatutako Cross-Site Scripting-en (XSS) aurrean. Erasotzaile batek URLren parametro jakin batzuk bidal litzake ahultasun hori baliatzeko. Ahultasun horretarako CVE-2019-5314 identifikatzailea erreserbatu da.
- ArubaOSren web kudeaketarako interfazeak duen komandoen injekzio erako ahultasuna baliatuz, autentifikatutako erasotzaile batek komando arbitrarioak exekuta litzake azpiko sistema eragilean. Asmo gaiztoko administratzaile batek gaitasun hori balia lezake atzeko ateak instalatzeko edo sistemaren konfigurazioa aldatzeko, erregistrorik gera ez dadin. Ahultasun honek ArubaOS 8.x bertsioei soilik eragiten die. Ahultasun horretarako CVE-2019-5315 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/09/26

Garrantzia: Altua

Kaltetutako baliabideak:

- Cisco IOS edo IOS XE-ren bertsio ahul bat exekutatzen duten eta Ident protokoloaren eskaerei erantzuteko konfiguratuta dauden Cisco produktuak.
- Cisco IOS XE softwarearen bertsio ahul bat exekutatzen duten Cisco Catalyst 3850 eta 9300 switch-ak.
- Cisco IOS XE softwarea, gailuak IPv6 helbide gaitu bat duen UTD interfazea badu eta gailua konfiguratuta badago Cisco UTD-ren Snort IPS funtzioarekin, URLan oinarritutako Cisco UTDren iragazki funtzioarekin edo biekin.
- Cisco IOS XE softwarearen bertsio ahul bat exekutatzen duten gailuak, NAT, NAT64 edo ZBFWrekin konfiguratuta badaude, eta FTP ikuskaritza gaituta.
- Ciscoren ondorengo produktuak, Cisco IOx aplikazioa ingurunearekin konfiguratuta badaude, eta konpondutako lehen bertsioa baino lehenagoko software bertsio bat exekutatzen badute:
  - Cisco 510 WPAN Industrial Router: Industrial Routers Operating System Software,
  - Cisco CGR 1000 Compute Module: CGR 1000 IOx Compute Platform Firmware,
  - Cisco IC3000 Industrial Compute Gateway: Industrial Compute Gateway Software,
  - Cisco Industrial Ethernet 4000 Series Switches: Cisco IOS Software.
- Cisco IOS XE Software-ren bertsio ahul bat exekutatzen duten Cisco gailuak.
- Cisco-ren ASR 900 serieko routerrak, Cisco IOS XE softwarearen 16.9 bertsioa badute eta Raw Socket TCP zerbitzari baten modura konfiguratuta badaude. Aukera hori ez dago gaituta modu lehenetsian.
- Cisco IOS edo IOS XEren bertsio ahul bat duten Cisco routerrak, ondoko funtzioetako edozein gaituta badute:
  - Cisco Unified Border Element (CUBE),
  - Cisco Unified Communications Manager Express (CME),
  - Cisco IOS Gateways with Session Initiation Protocol (SIP),
  - Cisco TDM Gateways,
  - Cisco Unified Survivable Remote Site Telephony (SRST),
  - Cisco Business Edition 4000 (BE4K).
- IOS XE softwarearen bertsio ahul bat duten Cisco gailuak, HTTP Server funtzioa aktibatuta badute.
- Cisco 800 Series Industrial Integrated Services Routers eta Cisco 1000 Series Connected Grid Routers (CGR 1000), Cisco IOS softwarearen bertsio ahul bat eta Guest OS instalatuta badute.
- Cisco IOS softwarearen bertsio ahul bat duten Cisco gailu hauek:
  - Cisco Catalyst 4500 Supervisor Engine 6-E,
  - Cisco Catalyst 4500 Supervisor Engine 6L-E,
  - Cisco Catalyst 4900M Switch,
  - Cisco Catalyst 4948E Ethernet Switch,
  - Cisco Catalyst 4948E-F Ethernet Switch.
- NATekin funtzionatzeko konfiguratuta dagoen Cisco IOS XE softwarearen bertsio ahul bat duten Cisco gailu hauek:
  - Cisco 1100, 4200, and 4300 Integrated Services Routers (ISRs),
  - Cisco Cloud Services Router (CSR) 1000V Series,
  - Cisco Enterprise Network Compute System (ENCS),
  - Cisco Integrated Services Virtual Router (ISRv).

Azalpena:

Ciscok bere produktuei eragiten dieten larritasun altuko 12 ahultasunen berri eman du.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Software Cisco-ren deskarga paneletik deskarga daitezke.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunen bat balia lezake honako ekintza hauetakoren bat egin ahal izateko:

- kaltetutako gailua birkargatu;
- asmo gaiztoko softwarearen irudi bat instalatu eta abiarazi edo sinatu gabeko bitarrak exekutatu;
- zerbitzuaren ukapena eragin;
- komandoak exekutatu administratzaile pribilegioekin edo gonbidatutako sistema eragilera (SO gonbidatua) baimenik gabeko sarbidea lortu.

Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2019-12647, CVE-2019-12649, CVE-2019-12657, CVE-2019-12655, CVE-2019-12656, CVE-2019-12658, CVE-2019-12653, CVE-2019-12654, CVE-2019-12650, CVE-2019-12651, CVE-2019-12648, CVE-2019-12652 eta CVE-2019-12646.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Ahultasuna Dell EMCren Data Protection Central Authentication-en

Argitalpen data: 2019/09/05

Garrantzia: Altua

Kaltetutako baliabideak:

- Dell EMC Data Protection Central 1.0,
- Dell EMC Data Protection Central 1.0.1,
- Dell EMC Data Protection Central 18.1,
- Dell EMC Data Protection Central 18.2,
- Dell EMC Data Protection Central 19.1.

Azalpena:

Dell EMC Data Protection Central-ek duen autentifikazio ahultasun bat baliatuz, erasotzaile batek arriskuan jar lezake kaltetutako sistema.

Konponbidea:

- Dell EMC Data Protection Central-en 18.2.1 eta 19.1.1 bertsioetara eguneratzea.

Xehetasuna:

Ziurtagiriaren konfiantzaren kate desegoki erako ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek Data Protection Central-eko CAk sinatutako ziurtagiri bat eskura lezake, eta horrela sistema baliagarri bat dela sinestaraz lezake eta datuen integritatea arriskuan jarri. Ahultasun horretarako CVE-2019-3762 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

WordPress-entzat 5.2.3 segurtasun eguneraketa

Argitalpen data: 2019/09/05

Garrantzia: Altua

Kaltetutako baliabideak:

WordPress, 5.2.2 eta lehenagoko bertsioak.

Azalpena:

62 ikertzaile baino gehiagok lankidetzan jardun dute hainbat ahultasun identifikatzen, bertsio honetan zuzendu direnak. 29 zuzenketa eta hobekuntza daude bertan, bai eta hainbat segurtasun zuzenketa ere.

Konponbidea:

Ahultasun horiek konpontzeko WordPress edukien kudeatzailearen 5.2.3 bertsioa argitaratu da, eta haien deskargen orrian eskuragarri dago.

Xehetasuna:

Segurtasun zuzenketek honako ahultasun hauek konpontzen dituzte:

- *Cross-Site Scripting* (XSS) lankideen argitalpenetako aurrebistetan, gordetako iruzkinetan eta kode laburtuen aurrebistetan, URL bat saneatzean gertatzen den arazo batengatik.
- Birbideratze irekia URL bat baliozkotzean eta saneatzean.
- XSS islatua multimedia edukia igotzen denean eta aginte taulan.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun Netgear-en produktuetan

Argitalpen data: 2019/09/05

Garrantzia: Altua

Kaltetutako baliabideak:

- Kaltetutako gailuak ondokoak dira:
  - D3600, firmwarearen 1.0.0.76 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D6000, firmwarearen 1.0.0.76 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D6220, firmwarearen 1.0.0.40 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D6220, firmwarearen 1.0.0.44 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D6400, firmwarearen 1.0.0.78 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D7000v2, firmwarearen 1.0.0.51 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D8500, firmwarearen 1.0.3.39 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D8500, firmwarearen 1.0.3.42 bertsioa baino lehenagokoak exekutatzen dituenean;
  - DGN2200v4, firmwarearen 1.0.0.110 bertsioa baino lehenagokoak exekutatzen dituenean;

- DGND2200Bv4, firmwarearen 1.0.0.110 bertsioa baino lehenagokoak exekutatzen dituenean;
- EX3700, firmwarearen 1.0.0.70 bertsioa baino lehenagokoak exekutatzen dituenean;
- EX3800, firmwarearen 1.0.0.70 bertsioa baino lehenagokoak exekutatzen dituenean;
- EX6000, firmwarearen 1.0.0.30 bertsioa baino lehenagokoak exekutatzen dituenean;
- EX6100, firmwarearen 1.0.2.22 bertsioa baino lehenagokoak exekutatzen dituenean;
- EX6100, firmwarearen 1.0.2.24 bertsioa baino lehenagokoak exekutatzen dituenean;
- EX6120, firmwarearen 1.0.0.40 bertsioa baino lehenagokoak exekutatzen dituenean;
- EX6130, firmwarearen 1.0.0.22 bertsioa baino lehenagokoak exekutatzen dituenean;
- EX6150v1, firmwarearen 1.0.0.42 bertsioa baino lehenagokoak exekutatzen dituenean;
- EX6200, firmwarearen 1.0.3.88 bertsioa baino lehenagokoak exekutatzen dituenean;
- EX7000, firmwarearen 1.0.0.66 bertsioa baino lehenagokoak exekutatzen dituenean;
- JNDR3000, firmwarearen 1.0.0.22 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6250, firmwarearen 1.0.4.26 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6300v2, firmwarearen 1.0.4.18 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6300v2, firmwarearen 1.0.4.22 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6300v2, firmwarearen 1.0.4.28 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6400, firmwarearen 1.0.1.24 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6400, firmwarearen 1.0.1.36 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6400v2, firmwarearen 1.0.2.32 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6400v2, firmwarearen 1.0.2.52 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6700, firmwarearen 1.0.1.22 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6700, firmwarearen 1.0.1.44 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6700, firmwarearen 1.0.1.46 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6700v3, firmwarearen 1.0.2.32 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6900, firmwarearen 1.0.1.22 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6900, firmwarearen 1.0.1.44 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6900, firmwarearen 1.0.1.46 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6900P, firmwarearen 1.0.0.56 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6900P, firmwarearen 1.3.1.26 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6900P, firmwarearen 1.3.1.64 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7000, firmwarearen 1.0.9.28 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7000, firmwarearen 1.0.9.6 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7000P, firmwarearen 1.0.0.56 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7000P, firmwarearen 1.3.1.26 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7000P, firmwarearen 1.3.1.64 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7100LG, firmwarearen 1.0.0.42 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7100LG, firmwarearen 1.0.0.46 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7300DST, firmwarearen 1.0.0.54 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7300DST, firmwarearen 1.0.0.62 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7300DST, firmwarearen 1.0.0.68 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7800, firmwarearen 1.0.2.60 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7900, firmwarearen 1.0.1.26 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7900, firmwarearen 1.0.2.10 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7900, firmwarearen 1.0.2.16 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7900P, firmwarearen 1.3.0.10 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7900P, firmwarearen 1.4.1.42 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8000, firmwarearen 1.0.4.12 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8000, firmwarearen 1.0.4.18 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8000P, firmwarearen 1.3.0.10 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8000P, firmwarearen 1.4.1.42 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8300, firmwarearen 1.0.2.106 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8300, firmwarearen 1.0.2.116 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8300, firmwarearen 1.0.2.122 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8500, firmwarearen 1.0.2.106 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8500, firmwarearen 1.0.2.116 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8500, firmwarearen 1.0.2.122 bertsioa baino lehenagokoak exekutatzen dituenean;
- WN2500RPv2, firmwarearen 1.0.1.54 bertsioa baino lehenagokoak exekutatzen dituenean;
- WNDR3400v3, firmwarearen 1.0.1.18 bertsioa baino lehenagokoak exekutatzen dituenean;
- WNDR3400v3, firmwarearen 1.0.1.22 bertsioa baino lehenagokoak exekutatzen dituenean;
- WNDR4500v2, firmwarearen 1.0.0.68 bertsioa baino lehenagokoak exekutatzen dituenean;
- WNR3500Lv2, firmwarearen 1.2.0.46 bertsioa baino lehenagokoak exekutatzen dituenean;
- WNR3500Lv2, firmwarearen 1.2.0.48 bertsioa baino lehenagokoak exekutatzen dituenean;
- WNR3500Lv2, firmwarearen 1.2.0.54 bertsioa baino lehenagokoak exekutatzen dituenean;
- XR500, firmwarearen 2.3.2.32 bertsioa baino lehenagokoak exekutatzen dituenean.

Azalpena:

Netgear-ek hainbat produkturi eragiten dieten kritikotasun altuko 10 ahultasun aurkitu ditu.

Konponbidea:

Netgear-en zerbitzu orrialdera sartzea eta kaltetutako gailuaren azken firmware bertsioa deskargatzea.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunen bat balia lezake honako ekintza hauetakoren bat egin ahal izateko:

- SQL injekzioa;
- bufferraren gainezkatzea;
- komandoen injekzioa.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Netgear-en produktuetan

Argitalpen data: 2019/09/05

Garrantzia: Altua

Kaltetutako baliabideak:

- Kaltetutako gailuak ondokoak dira:
  - D3600, firmwarearen 1.0.0.76 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D6000, firmwarearen 1.0.0.76 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D6220, firmwarearen 1.0.0.40 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D6220, firmwarearen 1.0.0.44 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D6400, firmwarearen 1.0.0.78 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D7000v2, firmwarearen 1.0.0.51 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D8500, firmwarearen 1.0.3.39 bertsioa baino lehenagokoak exekutatzen dituenean;
  - D8500, firmwarearen 1.0.3.42 bertsioa baino lehenagokoak exekutatzen dituenean;
  - DGN2200v4, firmwarearen 1.0.0.110 bertsioa baino lehenagokoak exekutatzen dituenean;
  - DGND2200Bv4, firmwarearen 1.0.0.110 bertsioa baino lehenagokoak exekutatzen dituenean;
  - EX3700, firmwarearen 1.0.0.70 bertsioa baino lehenagokoak exekutatzen dituenean;
  - EX3800, firmwarearen 1.0.0.70 bertsioa baino lehenagokoak exekutatzen dituenean;
  - EX6000, firmwarearen 1.0.0.30 bertsioa baino lehenagokoak exekutatzen dituenean;
  - EX6100, firmwarearen 1.0.2.22 bertsioa baino lehenagokoak exekutatzen dituenean;
  - EX6100, firmwarearen 1.0.2.24 bertsioa baino lehenagokoak exekutatzen dituenean;
  - EX6120, firmwarearen 1.0.0.40 bertsioa baino lehenagokoak exekutatzen dituenean;
  - EX6130, firmwarearen 1.0.0.22 bertsioa baino lehenagokoak exekutatzen dituenean;
  - EX6150v1, firmwarearen 1.0.0.42 bertsioa baino lehenagokoak exekutatzen dituenean;
  - EX6200, firmwarearen 1.0.3.88 bertsioa baino lehenagokoak exekutatzen dituenean;
  - EX7000, firmwarearen 1.0.0.66 bertsioa baino lehenagokoak exekutatzen dituenean;
  - JNDR3000, firmwarearen 1.0.0.22 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6250, firmwarearen 1.0.4.26 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6300v2, firmwarearen 1.0.4.18 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6300v2, firmwarearen 1.0.4.22 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6300v2, firmwarearen 1.0.4.28 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6400, firmwarearen 1.0.1.24 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6400, firmwarearen 1.0.1.36 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6400v2, firmwarearen 1.0.2.32 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6400v2, firmwarearen 1.0.2.52 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6700, firmwarearen 1.0.1.22 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6700, firmwarearen 1.0.1.44 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6700, firmwarearen 1.0.1.46 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6700v3, firmwarearen 1.0.2.32 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6900, firmwarearen 1.0.1.22 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6900, firmwarearen 1.0.1.44 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6900, firmwarearen 1.0.1.46 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6900P, firmwarearen 1.0.0.56 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6900P, firmwarearen 1.3.1.26 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R6900P, firmwarearen 1.3.1.64 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7000, firmwarearen 1.0.9.28 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7000, firmwarearen 1.0.9.6 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7000P, firmwarearen 1.0.0.56 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7000P, firmwarearen 1.3.1.26 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7000P, firmwarearen 1.3.1.64 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7100LG, firmwarearen 1.0.0.42 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7100LG, firmwarearen 1.0.0.46 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7300DST, firmwarearen 1.0.0.54 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7300DST, firmwarearen 1.0.0.62 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7300DST, firmwarearen 1.0.0.68 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7800, firmwarearen 1.0.2.60 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7900, firmwarearen 1.0.1.26 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7900, firmwarearen 1.0.2.10 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7900, firmwarearen 1.0.2.16 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7900P, firmwarearen 1.3.0.10 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R7900P, firmwarearen 1.4.1.42 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R8000, firmwarearen 1.0.4.12 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R8000, firmwarearen 1.0.4.18 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R8000P, firmwarearen 1.3.0.10 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R8000P, firmwarearen 1.4.1.42 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R8300, firmwarearen 1.0.2.106 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R8300, firmwarearen 1.0.2.116 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R8300, firmwarearen 1.0.2.122 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R8500, firmwarearen 1.0.2.106 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R8500, firmwarearen 1.0.2.116 bertsioa baino lehenagokoak exekutatzen dituenean;
  - R8500, firmwarearen 1.0.2.122 bertsioa baino lehenagokoak exekutatzen dituenean;
  - WN2500RPv2, firmwarearen 1.0.1.54 bertsioa baino lehenagokoak exekutatzen dituenean;
  - WNDR3400v3, firmwarearen 1.0.1.18 bertsioa baino lehenagokoak exekutatzen dituenean;
  - WNDR3400v3, firmwarearen 1.0.1.22 bertsioa baino lehenagokoak exekutatzen dituenean;
  - WNDR4500v2, firmwarearen 1.0.0.68 bertsioa baino lehenagokoak exekutatzen dituenean;
  - WNR3500Lv2, firmwarearen 1.2.0.46 bertsioa baino lehenagokoak exekutatzen dituenean;
  - WNR3500Lv2, firmwarearen 1.2.0.48 bertsioa baino lehenagokoak exekutatzen dituenean;
  - WNR3500Lv2, firmwarearen 1.2.0.54 bertsioa baino lehenagokoak exekutatzen dituenean;
  - XR500, firmwarearen 2.3.2.32 bertsioa baino lehenagokoak exekutatzen dituenean.

Azalpena:

Netgear-ek hainbat produkturi eragiten dieten kritikotasun altuko 10 ahultasun aurkitu ditu.

Konponbidea:

Netgear-en zerbitzu orrialdera sartzea eta kaltetutako gailuaren azken firmware bertsioa deskargatzea.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunen bat balia lezake honako ekintza hauetakoren bat egin ahal izateko:

- SQL injekzioa;
- bufferraren gainezkatzea;
- komandoen injekzioa.

Etiketak: Eguneraketa, Ahultasuna

Kodearen urruneko exekuzioa Exim-en

Argitalpen data: 2019/09/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

4.92tik 4.92.2ra bitarteko bertsio guztiak (biak barne).

Azalpena:

Memoria dinamikoan (heap) oinarritutako bufferraren gainezkatze erako ahultasun bat aurkitu da string_vformat-en (string.c). Hori baliatuz erasotzaile batek urrunetik kodea exekuta lezake.

Konponbidea:

4.92.3 bertsiora eguneratzea.

Xehetasuna:

string_vformat-ek (string.c) duen memoria dinamikoan (heap) oinarritutako bufferraren gainezkatze erako ahultasun bat baliatuz, erasotzaile batek kodea urrunetik exekuta lezake edo zerbitzuaren ukapen egoera eragin, ohi ez bezalako EHLO kate luze bat erabiliz, mezua jasotzen ari den Exim prozesua blokeatzeko. Ahultasun horretarako CVE-2019-16928 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun Netgear-en N300 WNR2000v5 gailuan

Argitalpen data: 2019/09/10

Garrantzia: Altua

Kaltetutako baliabideak:

Router Netgear N300 WNR2000v5, *firmware*-aren 1.0.0.70 bertsioa.

Azalpena:

Cisco Talos-eko Dave McDaniel-ek zerbitzuaren ukapen erako bi ahultasunen berri eman du, Netgear-en N300 WNR2000v5 haririk gabeko router-ari eragiten diotenak.

Konponbidea:

Netgear N300 WNR2000v5 1.0.0.72 bertsiora eguneratzea.

Xehetasuna:

- Netgear N300 WNR2000v5 produktuan zerbitzuaren ukapen erako ahultasun bat dago HTTP zerbitzariaren saioak kudeatzeko funtzionaltasunean. User-Agent katea hutsik duen HTTP eskari bat autentifikazioa behar duen orrialde batera bidaliz gero, erakusle huts bat ezabatzea gerta liteke, eta ondorioz HTTP zerbitzua blokeatuko litzateke. Autentifikatu gabeko erasotzaile batek bereziki diseinatutako HTTP eskari bat bidal dezake ahultasun hori aktibatzeko. Ahultasun horretarako CVE-2019-5054 identifikatzailea erreserbatu da.
- Zerbitzuaren ukapen erako ahultasun bat dago Netgear N300 WNR2000v5 haririk gabeko router-aren Host Access Point Daemon-en (hostapd).< *WFAWLANConfig:1#PutMessage* > zerbitzura sekuentzia baliogabe batean bidalitako SOAP eskaera batek erakusle huts baten deserreferentzia eragin dezake, eta ondorioz hostapd zerbitzuaren akats bat gertatuko litzateke. Autentifikatu gabeko erasotzaile batek bereziki diseinatutako SOAP eskari bat bidal dezake ahultasun hori aktibatzeko. Ahultasun horretarako CVE-2019-5055 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

SAPen 2019ko iraileko segurtasun eguneraketa

Argitalpen data: 2019/09/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa;
- SAP Business One Client, 9.2 eta 9.3 bertsioak;
- SAP Business One, 9.3 bertsioa;
- SAP BusinessObjects Business Intelligence Platform (CMC), 4.1, 4.2 eta 4.3 bertsioak;
- SAP BusinessObjects Business Intelligence Platform, 4.1 eta 4.2 bertsioak;
- SAP Diagnostic Agent (LM-Service), 7.20 bertsioa;
- SAP HANA Extended Application Services, 1.0.118 baino lehenagoko bertsioak;
- SAP HANA, 1.0 eta 2.0 bertsioak;
- SAP Kernel (RFC), honako bertsioak: KRNL32NUC, KRNL32UC eta KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73 eta KERNEL 7.21, 7.49, 7.53, 7.73, 7.76;
- Java (Web Container)-ENGINEAPIrako SAP NetWeaver AS, 7.10, 7.20, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
- SAP NetWeaver Process Integration Runtime Workbench - MESSAGING eta SAP_XIA, 7.31, 7.40 eta 7.50 bertsioak;
- SAP Supplier Relationship Management (Master Data Management Catalog) (SRM_MDM_CAT), 3.73, 7.31 eta 7.32 bertsioak.

Azalpena:

SAPek hainbat produkturi buruzko segurtasun eguneraketa batzuk argitaratu ditu bere hileroko komunikatuan.

Konponbidea:

SAPen zerbitzu ataria bisitatzea, eta fabrikatzaileak adierazten duen moduan beharrezkoak diren eguneraketa edo partxeak instalatzea.

Xehetasuna:

SAPek segurtasun partxeei buruz argitaratzen duen hileroko komunikatuan 4 segurtasun ohar eta 3 eguneraketa eman ditu ezagutzera. Horietatik 4 larritasun kritikokoak dira, 1 larritasun altukoa, 7 larritasun ertainekoak eta 1 larritasun baxukoa.

Argitaratutako ahultasun motak honako hauek dira:

- Sistema eragileko komandoen injekzio erako 2 ahultasun;
- zerbitzuaren ukapen erako 2 ahultasun;
- *Cross-Site Scripting* (XSS) erako 2 ahultasun;
- pribilegioen eskalatze erako ahultasun bat;
- kode injekzioko ahultasun bat;
- beste era batzuetako 5 ahultasun.

Kritikotzat eta altutzat kalifikatutako segurtasun oharrak honi buruzkoak dira:

- Erabiltzailearen sarreraren egiaztapenaren saiheste erako ahultasun bat. Erasotzaile batek kodea injekta lezake, web eduki dinamiko baten modukoa, eta komandoen baimenik gabeko exekuzioa eragin, informazio sentikorra ezagutzera eman edo zerbitzuaren ukapen egoera sortu. Ahultasun horretarako CVE-2019-0355 identifikatzailea erabili da.
- 2018ko apirileko buletinaren eguneraketa bat.
- 2019ko uztaileko buletinaren eguneraketa bat.
- Autentifikatutako erasotzaile batek zerbitzuaren ukapen egoera eragin lezake. Ahultasun horretarako CVE-2019-0364 identifikatzailea erabili da.

Etiketak: Eguneraketa, SAP, Ahultasuna

Hainbat ahultasun Moodle-n

Argitalpen data: 2019/09/17

Garrantzia: Altua

Kaltetutako baliabideak:

3.7tik 3.7.1era bitartekoak, 3.6tik 3.6.5era bitartekoak, 3.5etik 3.5.7ra bitartekoak, eta zerbitzurik gabeko lehenagoko bertsioak.

Azalpena:

Moodle plataforman 6 ahultasun aurkitu dira, 2 kritikotasun altukoak eta beste 4 kritikotasun baxukoak.

Konponbidea:

3.7.2, 3.6.6 eta 3.5.8 bertsioetara eguneratzea.

Xehetasuna:

- Kritikotasun altuko ahultasun bat baliatuz erasotzaile batek kodea injekta lezake hainbat txantiloitan. Ahultasun horretarako CVE-2019-14827 identifikatzailea erreserbatu da.
- Kritikotasun altuko ahultasun batek agerian utz lezake sarbide *token*-a, gailu mugikorrak erabiltzen dituzten erabiltzaileen kasuan. Horrek ez die eragiten app-a sarbide metodo modura erabiltzen duten erabiltzaileei, bortxatutako URL eskema konfiguratuta duten webguneei edo zerbitzu mugikorra desgaituta dutenei. Ahultasun horretarako CVE-2019-14830 identifikatzailea erreserbatu da.
- Larritasun baxuko gainerako ahultasunetarako ondoko identifikatzaileak erreserbatu dira: CVE-2019-14828, CVE-2019-14829 eta CVE-2019-14831.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun VMware produktuetan

Argitalpen data: 2019/09/20

Garrantzia: Altua

Kaltetutako baliabideak:

- VMware vSphere ESXi, 6.7, 6.5 eta 6.0 bertsioak;
- VMware Workstation Pro / Player, 15.x bertsioak;
- VMware Fusion Pro / Fusion, 11.x bertsioak;
- Windows eta Linux-erako VMware Remote Console (VMRC), 10.x bertsioak;
- Windows, Linux eta Mac-erako VMware Horizon Client, 5.x eta lehenagoko bertsioak.

Azalpena:

Hainbat ikertzailek 2 ahultasunen berri eman diote VMware-ri, bata larritasun altukoa eta bestea ertainekoa. Hurrenez hurren, bata memoria askatu ondoreneko erabilpen erakoa da, eta bestea zerbitzuaren ukapenekoa, eta VMware-ren hainbat produkturi eragiten diete.

Konponbidea:

- ESXi-n:
  - 6.7 bertsioa, ESXi670-201904101-SG partxea aplikatzea;

    - 6.5 bertsioa, ESXi650-201903401-SG partxea aplikatzea;
    - 6.0 bertsioa, ESXi600-201909101-SG partxea aplikatzea.
- Workstation 15.5.0 bertsiora eguneratzea.
- Fusion 11.5.0 bertsiora eguneratzea.
- VMRC 10.0.5 edo geroagoko bertsiora eguneratzea.
- Horizon Client 5.2.0 bertsiora eguneratzea.

Xehetasuna:

- ESXi, Workstation, Fusion, VMRC eta Horizon Client produktuek memoriaren askapenaren ondoreneko erabilpen erako ahultasun bat daukate soinu gailu birtualean. Ekipo gonbidatuan sarbide administratiborik ez lukeen erasotzaile lokal batek ahultasun hori balia lezake *host*-ean kodea exekutatzeko. Ahultasun horretarako CVE-2019-5527 identifikatzailea erreserbatu da.
- Workstation eta Fusion produktuak ahulak dira beren sarean egin litekeen zerbitzuaren ukapen erako eraso baten aurrean, IPv6 pakete jakin batzuen trataera desegokiagatik.Erasotzaile batek ahultasun hori balia lezake bereziki diseinatutako IPv6 pakete bat bidaliz, VMware-ren NATeko ekipo gonbidatu batetik, eta horrela VMware-ren NAT modua erabiltzen duten ekipo gonbidatu guztiei sarerako sarbidea eragotziko lieke. Ahultasun hau soilik balia daiteke VMNATerako IPv6 modua gaituta badago. Ahultasun horretarako CVE-2019-5535 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Hainbat ahultasun TIBCO produktuetan

Argitalpen data: 2019/09/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- R - Server Edition-erako TIBCO Enterprise Runtime, 1.2.0 eta lehenagoko bertsioak.
- AWS Marketplace-rako TIBCO Spotfire Analytics Platform, 10.4.0 eta 10.5.0 bertsioak.

Azalpena:

TIBCOk larritasun kritikoko bi ahultasun aurkitu ditu. Autentifikatu gabeko urruneko erasotzaile batek sarbidea saihets lezake, informazio konfidentziala ezagutzera eman edo kode arbitrarioa exekutatu.

Konponbidea:

TIBCOk eguneraketa sorta bat argitaratu du ahultasun horiek konpontzeko.

- R - Server Edition-erako TIBCO Enterprise Runtime, 12.0 edo lehengoko bertsioak, 12.1 edo goragoko bertsiora eguneratzea.
- AWS Marketplace-rako TIBCO Spotfire Analytics Platform, 10.4.0 eta 10.5.0 bertsioak, 10.5.1 edo goragoko bertsiora eguneratzea.

Xehetasuna:

- Ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek sarbidea saihets lezake, informazio konfidentziala ezagutzera eman edo sisteman kode arbitrarioa exekutatu. Ahultasun horretarako CVE-2019-11210 identifikatzailea erreserbatu da.
- Ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake, informazio konfidentziala ezagutzera eman edo sistema eragilearen kontrola hartu. Ahultasun horretarako CVE-2019-11211 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Informazioa agerian uztea F5-en BIG-IP ASM-n

Argitalpen data: 2019/09/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- BIG-IP ASM duen VIPRION, honako bertsioak:
    - 15.0.0,
    - 14.0.0 eta 14.1.0,
    - 13.1.0 - 13.1.1,
    - 12.1.0 - 12.1.4,
    - 11.6.1 - 11.6.4,
    - 11.5.2 - 11.5.9.

Azalpena:

F5-ek larritasun kritikoko ahultasun bat aurkitu du BIG-IP ASM duten VIPRION sistemetan.

Konponbidea:

- BIG-IP ASMren ondoko bertsioak eguneratzea:
    - 15.0.1,
    - 14.1.2,
    - 14.0.1,
    - 13.1.3,
    - 12.1.5,
    - 11.6.5,
    - 11.5.10.

Xehetasuna:

Ahultasunaren jatorria BIG-IP ASM duten VIPRION sistemen arazo bat da, kudeaketa interfazeak BIG-IP 14.1.0 baino lehenagoko bertsioetan dituztenak, edo "Port Lockdown" parametroa "Allow All" aukeran konfiguratuta daukatenak. Erasotzaile batek informazio

konfidentziala ezagutzera eman lezake, edo sistemaren konfigurazioa aldatu lehenetsitako ezarpenak erabiltzen ez direnean. Ahultasun horretarako CVE-2019-6650 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun VMware produktuetan

Argitalpen data: 2019/09/20

Garrantzia: Altua

Kaltetutako baliabideak:

- VMware vSphere ESXi, 6.7, 6.5 eta 6.0 bertsioak;
- VMware Workstation Pro / Player, 15.x bertsioak;
- VMware Fusion Pro / Fusion, 11.x bertsioak;
- Windows eta Linux-erako VMware Remote Console (VMRC), 10.x bertsioak;
- Windows, Linux eta Mac-erako VMware Horizon Client, 5.x eta lehenagoko bertsioak.

Azalpena:

Hainbat ikertzailek 2 ahultasunen berri eman diote VMware-ri, bata larritasun altukoa eta bestea ertainekoa. Hurrenez hurren, bata memoria askatu ondoreneko erabilpen erakoa da, eta bestea zerbitzuaren ukapenekoa, eta VMware-ren hainbat produkturi eragiten diete.

Konponbidea:

- ESXi-n:
  - 6.7 bertsioa, ESXi670-201904101-SG partxea aplikatzea;
  - 6.5 bertsioa, ESXi650-201903401-SG partxea aplikatzea;
  - 6.0 bertsioa, ESXi600-201909101-SG partxea aplikatzea.
- Workstation 15.5.0 bertsiora eguneratzea.
- Fusion 11.5.0 bertsiora eguneratzea.
- VMRC 10.0.5 edo geroagoko bertsiora eguneratzea.
- Horizon Client 5.2.0 bertsiora eguneratzea.

Xehetasuna:

- ESXi, Workstation, Fusion, VMRC eta Horizon Client produktuek memoriaren askapenaren ondoreneko erabilpen erako ahultasun bat daukate soinu gailu birtualean. Ekipo gonbidatuan sarbide administratiborik ez lukeen erasotzaile lokal batek ahultasun hori balia lezake *host*-ean kodea exekutatzeko. Ahultasun horretarako CVE-2019-5527 identifikatzailea erreserbatu da.
- Workstation eta Fusion produktuak ahulak dira beren sarean egin litekeen zerbitzuaren ukapen erako eraso baten aurrean, IPv6 pakete jakin batzuen trataera desegokiagatik.Erasotzaile batek ahultasun hori balia lezake bereziki diseinatutako IPv6 pakete bat bidaliz, VMware-ren NATeko ekipo gonbidatu batetik, eta horrela VMware-ren NAT modua erabiltzen duten ekipo gonbidatu guztiei sarerako sarbidea eragotziko lieke. Ahultasun hau soilik balia daiteke VMNATerako IPv6 modua gaituta badago. Ahultasun horretarako CVE-2019-5535 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Microsoft-en zikloz kanpoko hainbat ahultasun

Argitalpen data: 2019/09/24

Garrantzia: Altua

Kaltetutako baliabideak:

- Internet Explorer 11,
- Internet Explorer 10,
- Internet Explorer 9,
- Windows Defender,
- Microsoft Forefront Endpoint Protection 2010,
- Microsoft Security Essentials,
- Microsoft System Center 2012 Endpoint Protection,
- Microsoft System Center 2012 R2 Endpoint Protection,
- Microsoft System Center Endpoint Protection.

Azalpena:

Microsoft-ek kritikotasun altuak dituzten zikloz kanpoko bi ahultasun konpondu ditu. Urruneko erasotzaile batek kodea exekuta lezake edo zerbitzuaren ukapen egoera sortu.

Konponbidea:

Dagozkien segurtasun eguneraketak instalatzea. Eguneraketen instalazioari buruzko informazio orrian hori egiteko metodo ezberdinei buruzko argibideak daude.

Xehetasuna:

- Ahultasun baten jatorria da fitxategien kudeaketa desegoki bat Microsoft Defender-en. Sisteman exekuzio baimenak lituzkeen erasotzaile batek zerbitzuaren ukapen egoera eragin lezake. Ahultasun horretarako CVE-2019-1255 identifikatzailea erabili da.
- Beste ahultasunaren jatorria Internet Explorer-en *scripting* motorrak memoriako objektuak erabiltzeko duen modua da. Urruneko erasotzaile batek asmo gaiztoko webgune bat sor lezake kode arbitrarioa exekutatzeko edo sisteman erabiltzailearen pribilegioak lortzeko. Ahultasun horretarako CVE-2019-1367 identifikatzailea erabili da.

Etiketak: Eguneraketa, Microsoft, Nabigatzailea, Ahultasuna, Windows

Hainbat ahultasun VMware produktuetan

Argitalpen data: 2019/09/20

Garrantzia: Altua

Kaltetutako baliabideak:

- VMware vSphere ESXi, 6.7, 6.5 eta 6.0 bertsioak;
- VMware Workstation Pro / Player, 15.x bertsioak;
- VMware Fusion Pro / Fusion, 11.x bertsioak;
- Windows eta Linux-erako VMware Remote Console (VMRC), 10.x bertsioak;
- Windows, Linux eta Mac-erako VMware Horizon Client, 5.x eta lehenagoko bertsioak.

Azalpena:

Hainbat ikertzailek 2 ahultasunen berri eman diote VMware-ri, bata larritasun altukoa eta bestea ertainekoa. Hurrenez hurren, bata memoria askatu ondoreneko erabilpen erakoa da, eta bestea zerbitzuaren ukapenekoa, eta VMware-ren hainbat produkturi eragiten diete.

Konponbidea:

- ESXi-n:
  - 6.7 bertsioa, ESXi670-201904101-SG partxea aplikatzea;
  - 6.5 bertsioa, ESXi650-201903401-SG partxea aplikatzea;
  - 6.0 bertsioa, ESXi600-201909101-SG partxea aplikatzea.
- Workstation 15.5.0 bertsiora eguneratzea.
- Fusion 11.5.0 bertsiora eguneratzea.
- VMRC 10.0.5 edo geroagoko bertsiora eguneratzea.
- Horizon Client 5.2.0 bertsiora eguneratzea.

Xehetasuna:

- ESXi, Workstation, Fusion, VMRC eta Horizon Client produktuek memoriaren askapenaren ondoreneko erabilpen erako ahultasun bat daukate soinu gailu birtualean. Ekipo gonbidatuan sarbide administratiborik ez lukeen erasotzaile lokal batek ahultasun hori balia lezake *host*-ean kodea exekutatzeko. Ahultasun horretarako CVE-2019-5527 identifikatzailea erreserbatu da.
- Workstation eta Fusion produktuak ahulak dira beren sarean egin litekeen zerbitzuaren ukapen erako eraso baten aurrean, IPv6 pakete jakin batzuen trataera desegokiagatik.Erasotzaile batek ahultasun hori balia lezake bereziki diseinatutako IPv6 pakete bat bidaliz, VMware-ren NATeko ekipo gonbidatu batetik, eta horrela VMware-ren NAT modua erabiltzen duten ekipo gonbidatu guztiei sarerako sarbidea eragotziko lieke. Ahultasun hau soilik balia daiteke VMNATerako IPv6 modua gaituta badago. Ahultasun horretarako CVE-2019-5535 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

F5en hainbat produkturen REST framework-en ahultasuna

Argitalpen data: 2019/09/25

Garrantzia: Altua

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), honako bertsio hauek:
  - 15.0.0,
  - 14.0.0 - 14.1.0,
  - 13.1.0 - 13.1.1,
  - 12.1.0 - 12.1.4,
  - 11.5.2 - 11.6.4.
- Enterprise Manager, 3.1.1 bertsioa.
- BIG-IQ Centralized Management, honako bertsioak:
  - 7.0.0,
  - 6.0.0 - 6.1.0,
  - 5.2.0 - 5.4.0.
- F5 iWorkflow 2.3.0 bertsioa.

Azalpena:

Vingroup taldearen enpresa subsidiarioa den VINCSSeko Enter of the Tarantula ekipoak, F5ekin koordinazioan, kritikotasun altuko ahultasun bat aurkitu du REST framework osagaian. Erasotzaile batek sistema arriskuan jar lezake.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator):
  - 15.0.1,
  - 14.1.2,
  - 14.0.1,
  - 13.1.3,
  - 12.1.5,
  - 11.6.5.

Arintze neurri modura, kaltetutako gainerako produktuetarako eguneraketarik ez dago eskuragarri une honetan. F5ek kaltetutako sistemetan sare seguruak erabiltzea eta sarbidea konfiantzako erabiltzaileei soilik baimentzea gomendatzen du.

Xehetasuna:

Ahultasunaren jatorria saio hasierako sendotasunik gabeko HTTP erantzunak dira, eskaera aldatuak prozesatzen direnean. Erasotzaile batek asmo gaiztoko eskaerak bidal litzake sisteman ahultasunak baliatzeko. Ahultasun horretarako CVE-2019-6651 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Urruneko exekuzio erako ahultasuna e2fsprogs-en

Argitalpen data: 2019/09/25

Garrantzia: Altua

Kaltetutako baliabideak:

E2fsprogs, 1.45.4 baino lehenagoko bertsioak.

Azalpena:

Cisco Talos-eko Lilith ikertzaileak kodearen exekuzio erako larritasun altuko ahultasun bat aurkitu du e2fsprogs-en, ext2, ext3 eta ext4 fitxategien sistemen mantenurako utilitateen pakete bat.

Konponbidea:

e2fsprogs 1.45.4 bertsiora eguneratzea.

Xehetasuna:

Bereziki sortutako ext4 partizioen sistema batek mugez kanpoko idazketa eragin lezake memoria dinamikoan (*heap*), e2fsck-ek erabiltzen duen *quota* funtzionaltasunean. Erasotzaile batek kode arbitrarioa exekuta lezake sisteman. Ahultasun horretarako CVE-2019-5094 identifikatzailea erabili da.

Etiketak: Eguneraketa, Linux, Ahultasuna

Joomla! 3.9.12ren segurtasun eguneraketa

Argitalpen data: 2019/09/25

Garrantzia: Txikia

Kaltetutako baliabideak:

Joomla! CMS, 3.0.0tik 3.9.11ra bitarteko bertsioak.

Azalpena:

Joomla!-k bertsio berri bat argitaratu du, bere nukleoak duen *cross-site scripting* (XSS) erako kritikotasun txikiko ahultasun bat konpontzen duena.

Konponbidea:

3.9.12 bertsiora eguneratzea.

Xehetasuna:

Lehenetsitako txantiloietako *logo* parametroak zuen ahultasun bat baliatuz kodearen ihesaldi bat gerta liteke, eta horrela XSS bat eragin. Ahultasun horretarako CVE-2019-16725 identifikatzailea erabili da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/09/26

Garrantzia: Altua

Kaltetutako baliabideak:

- Cisco IOS edo IOS XE-ren bertsio ahul bat exekutatzen duten eta Ident protokoloaren eskaerei erantzuteko konfiguratuta dauden Cisco produktuak.
- Cisco IOS XE softwarearen bertsio ahul bat exekutatzen duten Cisco Catalyst 3850 eta 9300 switch-ak.
- Cisco IOS XE softwarea, gailuak IPv6 helbide gaitu bat duen UTD interfazea badu eta gailua konfiguratuta badago Cisco UTD-ren Snort IPS funtzioarekin, URLan oinarritutako Cisco UTDren iragazki funtzioarekin edo biekin.
- Cisco IOS XE softwarearen bertsio ahul bat exekutatzen duten gailuak, NAT, NAT64 edo ZBFWrekin konfiguratuta badaude, eta FTP ikuskaritza gaituta.
- Ciscoren ondorengo produktuak, Cisco IOx aplikazioa inguruneakin konfiguratuta badaude, eta konpondutako lehen bertsioa baino lehenagoko software bertsio bat exekutatzen badute:
  - Cisco 510 WPAN Industrial Router: Industrial Routers Operating System Software,
  - Cisco CGR 1000 Compute Module: CGR 1000 IOx Compute Platform Firmware,
  - Cisco IC3000 Industrial Compute Gateway: Industrial Compute Gateway Software,
  - Cisco Industrial Ethernet 4000 Series Switches: Cisco IOS Software.
- Cisco IOS XE Software-ren bertsio ahul bat exekutatzen duten Cisco gailuak.

- Cisco-ren ASR 900 serieko routerrak, Cisco IOS XE softwarearen 16.9 bertsioa badute eta Raw Socket TCP zerbitzari baten modura konfiguratuta badaude. Aukera hori ez dago gaituta modu lehenetsian.
- Cisco IOS edo IOS XEren bertsio ahul bat duten Cisco routerrak, ondoko funtzioetako edozein gaituta badute:
  - Cisco Unified Border Element (CUBE),
  - Cisco Unified Communications Manager Express (CME),
  - Cisco IOS Gateways with Session Initiation Protocol (SIP),
  - Cisco TDM Gateways,
  - Cisco Unified Survivable Remote Site Telephony (SRST),
  - Cisco Business Edition 4000 (BE4K).
- IOS XE softwarearen bertsio ahul bat duten Cisco gailuak, HTTP Server funtzioa aktibatuta badute.
- Cisco 800 Series Industrial Integrated Services Routers eta Cisco 1000 Series Connected Grid Routers (CGR 1000), Cisco IOS softwarearen bertsio ahul bat eta Guest OS instalatuta badute.
- Cisco IOS softwarearen bertsio ahul bat duten Cisco gailu hauek:
  - Cisco Catalyst 4500 Supervisor Engine 6-E,
  - Cisco Catalyst 4500 Supervisor Engine 6L-E,
  - Cisco Catalyst 4900M Switch,
  - Cisco Catalyst 4948E Ethernet Switch,
  - Cisco Catalyst 4948E-F Ethernet Switch.
- NATekin funtzionatzeko konfiguratuta dagoen Cisco IOS XE softwarearen bertsio ahul bat duten Cisco gailu hauek:
  - Cisco 1100, 4200, and 4300 Integrated Services Routers (ISRs),
  - Cisco Cloud Services Router (CSR) 1000V Series,
  - Cisco Enterprise Network Compute System (ENCS),
  - Cisco Integrated Services Virtual Router (ISRv).

Azalpena:

Ciscok bere produktuei eragiten dieten larritasun altuko 12 ahultasunen berri eman du.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Software Cisco-ren deskarga paneletik deskarga daitezke.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunen bat balia lezake honako ekintza hauetakoren bat egin ahal izateko:

- kaltetutako gailua birkargatu;
- asmo gaiztoko softwarearen irudi bat instalatu eta abiarazi edo sinatu gabeko bitarrak exekutatu;
- zerbitzuaren ukapena eragin;
- komandoak exekutatu administratzaile pribilegioekin edo gonbidatutako sistema eragilera (SO gonbidatua) baimenik gabeko sarbidea lortu.

Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2019-12647, CVE-2019-12649, CVE-2019-12657, CVE-2019-12655, CVE-2019-12656, CVE-2019-12658, CVE-2019-12653, CVE-2019-12654, CVE-2019-12650, CVE-2019-12651, CVE-2019-12648, CVE-2019-12652 eta CVE-2019-12646.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Kodearen urruneko exekuzioa Exim-en

Argitalpen data: 2019/09/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

4.92tik 4.92.2ra bitarteko bertsio guztiak (biak barne).

Azalpena:

Memoria dinamikoan (heap) oinarritutako bufferraren gainezkatze erako ahultasun bat aurkitu da string_vformat-en (string.c). Hori baliatuz erasotzaile batek urrunetik kodea exekuta lezake.

Konponbidea:

4.92.3 bertsiora eguneratzea.

Xehetasuna:

string_vformat-ek (string.c) duen memoria dinamikoan (heap) oinarritutako bufferraren gainezkatze erako ahultasun bat baliatuz, erasotzaile batek kodea urrunetik exekuta lezake edo zerbitzuaren ukapen egoera eragin, ohi ez bezalako EHLO kate luze bat erabiliz, mezua jasotzen ari den Exim prozesua blokeatzeko. Ahultasun horretarako CVE-2019-16928 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/09/26

Garrantzia: Altua

Kaltetutako baliabideak:

- Cisco IOS edo IOS XE-ren bertsio ahul bat exekutatzen duten eta Ident protokoloaren eskaerei erantzuteko konfiguratuta dauden Cisco produktuak.
- Cisco IOS XE softwarearen bertsio ahul bat exekutatzen duten Cisco Catalyst 3850 eta 9300 switch-ak.
- Cisco IOS XE softwarea, gailuak IPv6 helbide gaitu bat duen UTD interfazea badu eta gailua konfiguratuta badago Cisco UTD-ren

Snort IPS funtzioarekin, URLan oinarritutako Cisco UTDren iragazki funtzioarekin edo biekin.
- Cisco IOS XE softwarearen bertsio ahul bat exekutatzen duten gailuak, NAT, NAT64 edo ZBFWrekin konfiguratuta badaude, eta FTP ikuskaritza gaituta.
- Ciscoren ondorengo produktuak, Cisco IOx aplikazioa ingurunearekin konfiguratuta badaude, eta konpondutako lehen bertsioa baino lehenagoko software bertsio bat exekutatzen badute:
    - Cisco 510 WPAN Industrial Router: Industrial Routers Operating System Software,
    - Cisco CGR 1000 Compute Module: CGR 1000 IOx Compute Platform Firmware,
    - Cisco IC3000 Industrial Compute Gateway: Industrial Compute Gateway Software,
    - Cisco Industrial Ethernet 4000 Series Switches: Cisco IOS Software.
- Cisco IOS XE Software-ren bertsio ahul bat exekutatzen duten Cisco gailuak.
- Cisco-ren ASR 900 serieko routerrak, Cisco IOS XE softwarearen 16.9 bertsioa badute eta Raw Socket TCP zerbitzari baten modura konfiguratuta badaude. Aukera hori ez dago gaituta modu lehenetsian.
- Cisco IOS edo IOS XEren bertsio ahul bat duten Cisco routerrak, ondoko funtzioetako edozein gaituta badute:
    - Cisco Unified Border Element (CUBE),
    - Cisco Unified Communications Manager Express (CME),
    - Cisco IOS Gateways with Session Initiation Protocol (SIP),
    - Cisco TDM Gateways,
    - Cisco Unified Survivable Remote Site Telephony (SRST),
    - Cisco Business Edition 4000 (BE4K).
- IOS XE softwarearen bertsio ahul bat duten Cisco gailuak, HTTP Server funtzioa aktibatuta badute.
- Cisco 800 Series Industrial Integrated Services Routers eta Cisco 1000 Series Connected Grid Routers (CGR 1000), Cisco IOS softwarearen bertsio ahul bat eta Guest OS instalatuta badute.
- Cisco IOS softwarearen bertsio ahul bat duten Cisco gailu hauek:
    - Cisco Catalyst 4500 Supervisor Engine 6-E,
    - Cisco Catalyst 4500 Supervisor Engine 6L-E,
    - Cisco Catalyst 4900M Switch,
    - Cisco Catalyst 4948E Ethernet Switch,
    - Cisco Catalyst 4948E-F Ethernet Switch.
- NATekin funtzionatzeko konfiguratuta dagoen Cisco IOS XE softwarearen bertsio ahul bat duten Cisco gailu hauek:
    - Cisco 1100, 4200, and 4300 Integrated Services Routers (ISRs),
    - Cisco Cloud Services Router (CSR) 1000V Series,
    - Cisco Enterprise Network Compute System (ENCS),
    - Cisco Integrated Services Virtual Router (ISRv).

Azalpena:

Ciscok bere produktuei eragiten dieten larritasun altuko 12 ahultasunen berri eman du.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Software Cisco-ren deskarga paneletik deskarga daitezke.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunen bat balia lezake honako ekintza hauetakoren bat egin ahal izateko:

- kaltetutako gailua birkargatu;
- asmo gaiztoko softwarearen irudi bat instalatu eta abiarazi edo sinatu gabeko bitarrak exekutatu;
- zerbitzuaren ukapena eragin;
- komandoak exekutatu administratzaile pribilegioekin edo gonbidatutako sistema eragilera (SO gonbidatua) baimenik gabeko sarbidea lortu.

Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2019-12647, CVE-2019-12649, CVE-2019-12657, CVE-2019-12655, CVE-2019-12656, CVE-2019-12658, CVE-2019-12653, CVE-2019-12654, CVE-2019-12650, CVE-2019-12651, CVE-2019-12648, CVE-2019-12652 eta CVE-2019-12646.

Etiketak: Eguneraketa, Cisco, Ahultasuna