2019ko Abenduaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun Liferay-n

Argitalpen data: 2019/12/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Liferay Portal, 7.2.0 bertsioa eta lehenagokoak.

Azalpena:

6 ahultasun aurkitu dira, horietako bat larritasun kritikokoa eta beste bost larritasun altukoak. Urruneko erasotzaile batek erabiltzaile kredentzialak eskura litzake, kodea exekutatu edo injektatu, zerbitzuaren ukapen egoera eragin (Dos) edo sistemaren baliabideen gainean baimenik gabeko ekintzak egin.

Konponbidea:

Liferay Portal 7.2.1 bertsiora edo berriago batera eguneratzea, eskuragarri dagoenean.

Xehetasuna:

- Larritasun kritikoko ahultasuna baliatuz urruneko erasotzaile batek kodea exekuta lezake JSON web services (JSONWS) bitartez.
- Larritasun altuko ahultasunen jatorriak honakoak dira:
  - «*Sing In*» widget-ak duen akats batek ezagutzera eman litzake erabiltzailearen kredentzialak HTLMan.
  - Kontuaren Ezarpenetan (*Account Settings*) birbideratze irekiko ahultasun bat.
  - JSONWS */user/send-password-by-** APIa erabil liteke postaren zerbitzarian zerbitzuaren ukapen egoera sortzeko.
  - baimenetan dauden hainbat akats baliatuz erabiltzaileek baimenik gabeko ekintzak egin litzakete sistemaren baliabideen gainean.
  - *Cross-site-scripting* (XSS) erako hainbat ahultasun baliatuz kodea injekta liteke.

Etiketak: CMS, Ahultasuna

Hainbat ahultasun Netgear-en produktuetan

Argitalpen data: 2019/12/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- D3600, 1.0.0.76 bertsioa baino lehenagokoak;
- D6000, 1.0.0.76 bertsioa baino lehenagokoak;
- D6200, 1.1.00.36 bertsioa baino lehenagokoak;
- D7000, 1.0.1.74 bertsioa baino lehenagokoak;
- D7000v2, 1.0.0.53 bertsioa baino lehenagokoak;
- DM200, 1.0.0.58 bertsioa baino lehenagokoak;
- EX3700, 1.0.0.70 bertsioa baino lehenagokoak;
- EX3800, 1.0.0.70 bertsioa baino lehenagokoak;
- EX6000, 1.0.0.30 bertsioa baino lehenagokoak;
- EX6100, 1.0.2.24 bertsioa baino lehenagokoak;
- EX6120, 1.0.0.40 bertsioa baino lehenagokoak;
- EX6130, 1.0.0.22 bertsioa baino lehenagokoak;
- EX6150v1, 1.0.0.42 bertsioa baino lehenagokoak;
- EX6200, 1.0.3.88 bertsioa baino lehenagokoak;
- EX7000, 1.0.0.66 bertsioa baino lehenagokoak;
- JR6150, 1.0.1.24 bertsioa baino lehenagokoak;

- MR1100, 12.06.08.00 bertsioa baino lehenagokoak;
- PR2000, 1.0.0.28 bertsioa baino lehenagokoak;
- R6020, 1.0.0.42 bertsioa baino lehenagokoak;
- R6050, 1.0.1.24 bertsioa baino lehenagokoak;
- R6080, 1.0.0.42 bertsioa baino lehenagokoak;
- R6120, 1.0.0.48 bertsioa baino lehenagokoak;
- R6220, 1.1.0.86 bertsioa baino lehenagokoak;
- R6230, 1.1.0.86 bertsioa baino lehenagokoak;
- R6260, 1.1.0.64 bertsioa baino lehenagokoak;
- R6700, 1.0.2.6 bertsioa baino lehenagokoak;
- R6700v2, 1.2.0.62 bertsioa baino lehenagokoak;
- R6800, 1.2.0.62 bertsioa baino lehenagokoak;
- R6900, 1.0.2.4 bertsioa baino lehenagokoak;
- R6900P, 1.3.1.64 bertsioa baino lehenagokoak;
- R6900v2, 1.2.0.62 bertsioa baino lehenagokoak;
- R7000, 1.0.9.60 bertsioa baino lehenagokoak;
- R7000P, 1.3.1.64 bertsioa baino lehenagokoak;
- R7800, 1.0.2.60 bertsioa baino lehenagokoak;
- R7900, 1.0.3.8 bertsioa baino lehenagokoak;
- R7900P, 1.4.1.30 bertsioa baino lehenagokoak;
- R8000, 1.0.4.46 bertsioa baino lehenagokoak;
- R8000P, 1.4.1.30 bertsioa baino lehenagokoak;
- R8300, 1.0.2.128 bertsioa baino lehenagokoak;
- R8500, 1.0.2.128 bertsioa baino lehenagokoak;
- R8900, 1.0.4.12 bertsioa baino lehenagokoak;
- R9000, 1.0.4.12 bertsioa baino lehenagokoak;
- RAX40, 1.0.3.64 bertsioa baino lehenagokoak;
- WAC505, 8.2.1.16 bertsioa baino lehenagokoak;
- WAC510, 8.2.1.16 bertsioa baino lehenagokoak;
- WN2500RPv2, 1.0.1.54 bertsioa baino lehenagokoak;
- WNR2000v5, 1.0.0.72 bertsioa baino lehenagokoak;
- WNR2020, 1.1.0.62 bertsioa baino lehenagokoak;
- WNR614, 1.1.0.54 bertsioa baino lehenagokoak;
- XR500, 2.3.2.56 bertsioa baino lehenagokoak;
- XR700, 1.0.1.20 bertsioa baino lehenagokoak.

Azalpena:

Netgear-ek bere produktuei eragiten dieten 21 ahultasunen berri eman du, bat larritasun kritikokoa eta 20 larritasun altukoak.

Konponbidea:

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

Xehetasuna:

- Larritasun kritikoko ahultasuna baliatuz, erasotzaile batek kaltetutako gailuaren autentifikazioa saihets lezake.
- Larritasun altuko ahultasunak baliatuz, erasotzaile batek ondoko ekintzak egin litzake:
  - CSRF (*Cross Site Request Forgery*),
  - autentifikazioari ihes egitea,
  - bufferraren gainezkatzea autentifikazioaren aurretik,
  - pilaren gainezkatzea autentifikazioaren aurretik,
  - baimenik gabeko sarbidea,
  - komandoen injekzioa autentifikazioaren ondoren,
  - bufferraren gainezkatzea autentifikazioaren ondoren,
  - zerbitzuaren ukapen egoera eragitea,
  - informazioa sentikorra zabaltzea,
  - administratzailearen kredentzialak hedatzea.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Autentifikazioaren egiaztatze desegokia Palo Alto PAN-OSen

Argitalpen data: 2019/12/05

Garrantzia: Altua

Kaltetutako baliabideak:

- PAN-OS 7.1, 7.1.25 baino lehenagoko bertsioak;
- PAN-OS 8.0, 8.0.20 baino lehenagoko bertsioak;
- PAN-OS 8.1, 8.1.11 baino lehenagoko bertsioak;
- PAN-OS 9.0, 9.0.5 baino lehenagoko bertsioak.

Azalpena:

Palo Alto-k PAN-OSek duen ahultasun baten berri eman du. Hori baliatuz erasotzaile batek pribilegioak eskala litzake.

Konponbidea:

7.1.25, 8.0.20, 8.1.11, 9.0.5 edo geroagoko bertsioetara eguneratzea.

Xehetasuna:

Palo Alto Networks-en PAN-OSek duen autentifikazio egiaztapen desegoki bat baliatuz, baimen murriztuko rol pertsonalizatua lukeen erasotzaile batek pribilegioak eskala litzake eta supererabiltzaile bihurtu. Arazo honek soilik eragiten die aipatutako rolarekin konfiguratuta dauden gailuei. Ahultasun horretarako CVE-2019-17437 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Lehenetsitako IPMI kontua IBMren DataPower Gateway-n

Argitalpen data: 2019/12/10

Garrantzia: Altua

Kaltetutako baliabideak:

IBM DataPower Gateway, 2018.4.1.0-2018.4.1.5 eta 7.6.0.0-7.6.0.14 bertsioak.

Azalpena:

LAN-en gainean IPMI aukera aktibatzen denean, era berean automatikoki gaitzen da administratzaile kontua modu lehenetsian.

Konponbidea:

Honako hauetara eguneratzea:

- IBM DataPower Gateway 2018.4.1.6 (APAR IT29004);
- IBM DataPower Gateway 7.6.0.15 (APAR IT29004);

Xehetasuna:

IBM DataPower Appliance-k eta IBM MQ Appliance-k lehenetsitako administratzaile kontu bat daukate, aktibatu egiten dena LAN IPMI kanala aktibatuta badago. Urruneko erasotzaile batek kontu hori balia lezake BMCra baimenik gabeko sarbidea lortzeko. Ahultasun horretarako CVE-2019-4621 identifikatzailea erabili da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Urruneko exekuzio erako ahultasuna VMware produktuetan

Argitalpen data: 2019/12/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- VMware ESXi, honako bertsioak:
  - 6.7,
  - 6.5,
  - 6.0.
- VMware Horizon DaaS, 8.x bertsioen adarra.

Azalpena:

Tianfu Cup Pwn Contest 2019 lehiaketako 360Vulcan ekipoak VMware-ren hainbat produkturi eragiten dien larritasun kritikoko ahultasun bat aurkitu du. Urruneko erasotzaile batek kodea exekuta lezake sisteman.

Konponbidea:

- VMwarek hainbat segurtasun partxe argitaratu ditu VMware ESXi-rako, kaltetutako bertsioaren arabera:
  - 6.7 bertsioaren kasuan, ESXi670-201912001 partxea aplikatzea.
  - 6.5 bertsioaren kasuan, ESXi650-201912001 partxea aplikatzea.
  - 6.0 bertsioaren kasuan, ESXi600-201912001 partxea aplikatzea.
- Horizon DaaS-en kasuan, Hotfix-en serie bat argitaratu da ahultasuna arintzeko, hori konpontzeko eguneraketa bat argitaratzen den bitartean.

Xehetasuna:

OpenSLP zerbitzuak duen memoria dinamikoaren (heap) gainidazketa erako ahultasun bat baliatuz, 247 atakara sarbidea lukeen urruneko erasotzaile batek kodea exekuta lezake sisteman. Ahultasun horretarako CVE-2019-5544 identifikatzailea erabili da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Hainbat ahultasun Dell EMCren produktuetan

Argitalpen data: 2019/12/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Dell EMC Data Protection Advisor, honako bertsioak:
  - 6.3;
  - 6.4;
  - 6.5;
  - 18.1;
  - patch 83 baino lehenagoko 18.2;

    - patch 71 baino lehenagoko 19.1.
- Integrated Data Protection Appliance, honako bertsioak:
    - 2.0;
    - 2.1;
    - 2.2;
    - 2.3;
    - 2.4.

Azalpena:

DPA aplikazioaren API REST-ak, Dell EMC Data Protection Advisor-en softwarearen barnean, zuzenketak ditu hainbat ahultasunetarako, kaltetutako sistema arriskuan jartzeko baliatuak izan litezkeenak erasotzaileen aldetik.

Konponbidea:

Dell EMCren zerbitzu atarian erregistratutako erabiltzaileek ondoren zerrendatzen diren bertsioak deskarga ditzakete ahultasunak zuzentzeko:

- Dell EMC Data Protection Advisor, honako bertsioak:
    - 19.2;
    - patch 71 edo ondorengoa duen 19.1;
    - patch 83 edo ondorengoa duen 18.2;
    - 6.3, 6.4, 6.5, edo 18.1 bertsioen kasuan:18.2 bertsioko patch 83 edo berriagora eguneratzea, edo 19.1 bertsioko patch 71 edo berriagora.
- Integrated Data Protection Appliance:
    - 2.0, 2.1 edo 2.2 bertsioen kasuan:2.3 bertsiora eguneratzea eta Dell EMC Data Protection Advisor-en 18.2 bertsioko patch 83 edo berriagora eguneratzea;
    - 2.3 edo 2.4 bertsioen kasuan:Dell EMC Data Protection Advisor-en 18.2 bertsioko patch 83 edo berriagora eguneratzea.

Xehetasuna:

- Autentifikazio gabezi erako ahultasuna dago API RESTen zerbitzarian. Pribilegio administratiboak lituzkeen asmo gaiztoko urruneko erabiltzaile batek ahultasun hau balia lezake aplikazioko sistema eragileko komandoen zerrenda baimendua aldatzeko. Horren ondorioz sistema eragilearen komandoen exekuzio arbitrarioa gerta liteke, erabiltzaile normalak DPA zerbitzua kaltetutako sisteman exekutatzen baitu. Ahultasun horretarako CVE-2019-18581 identifikatzailea erreserbatu da.
- Txantiloiaren injekzio erako ahultasuna aurkitu da API RESTeko zerbitzariaren aldean. Pribilegio administratiboak lituzkeen asmo gaiztoko urruneko erabiltzaile batek ahultasun hau balia lezake zerbitzarian asmo gaiztoko txostenak sortzeko script-ak injektatzeko. Horren ondorioz sistema eragilearen komandoen exekuzioa gerta liteke, erabiltzaile normalak DPA zerbitzua kaltetutako produktuan exekutatzen baitu. Ahultasun horretarako CVE-2019-18582 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasunak Intel-en hainbat produktutan

Argitalpen data: 2019/12/11

Garrantzia: Altua

Kaltetutako baliabideak:

- Intel(R) Network Adapters-erako Linuxen Tresna Administratzaileak, 24.3 baino lehenagoko bertsioak.
- Intel Coreren 6., 7., 8., 9. eta 10. belaunaldiko prozesadoreak.
- Intel Xeon prozesadoreak, familia hauetakoak:
-
    - E3 v5 eta v6,
    - E-2100,
    - E-2200.
- Intel NUC 8:
    - Mainstream Game Kit,
    - Mainstream Game Mini Computer,
    - Home - NUC8i3CYSM.
- Intel NUC Kit:
    - NUC8i7BEK,
    - NUC8i7HNK,
    - NUC7i7DNKE,
    - NUC7i5DNKE,
    - NUC7i3DNHE,
    - NUC6i7KYK,
    - NUC6i5SYH,
    - NUC7CJYH,
    - NUC6CAYS.
- Intel Compute Card:
    - CD1P64GK,
    - CD1M3128MK,
    - CD1IV128MK.
- Intel Compute Stick:
    - STK2mv64CC,
    - STK2m3W64CC.
- Intel NUC Board:
    - DE3815TYBE,
    - D34010WYB.

Azalpena:

Intel-ek kritikotasun altuko zazpi ahultasun aurkitu ditu hainbat produktutan. Erasotzaile lokal batek pribilegioen eskalatzea egin lezake edo informazio sentikorra ezagutzera eman.

Konponbidea:

- Intel(R) Network Adapters-erako Linuxen Tresna Administratzaileen kasuan, 24.3 bertsiora edo berriago batera eguneratu.
- Kaltetutako prozesadore familien kasuan, Intelek gomendatzen du BIOSa eguneratzea eskuragarri dagoen azken bertsiora.

- Intel NUCen familien kasuan, eskuragarri dagoen *firmwarea*ren azken bertsiora eguneratzea. Informazio gehiago eskuratzeko "Erreferentziak" atala irakur daiteke.

Xehetasuna:

- Intel(R) Network Adapters-erako Linuxen Tresna Administratzaileetan memoriak duen babes ez-nahikoa baliatuz, autentifikatutako erasotzaile lokal batek pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2019-0159 identifikatzailea erreserbatu da.
- Intelen hainbat prozesadorek dituzten tentsioaren ezarpenen egiaztapen desegoki batzuk baliatuz, autentifikatutako erasotzaile lokal batek pribilegioen eskalatzea egin lezake edo informazioa ezagutzera eman. Ahultasun horretarako CVE-2019-11157 identifikatzailea erreserbatu da.
- Intel NUC-en ahultasunak:
-
    - Bufferraren murrizpen desegokiak baliatuz, autentifikatu gabeko erasotzaile lokal batek pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2019-14608 identifikatzailea erreserbatu da.
    - Sarbidearen kontrol desegoki bat baliatuz, autentifikatu gabeko erasotzaile lokal batek pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2019-14610 identifikatzailea erreserbatu da.
    - Sarrera parametroen baliozkotze desegoki bat baliatuz, pribilegioak lituzkeen erasotzaile lokal batek pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2019-14609 identifikatzailea erreserbatu da.
    - Osokoen gainezkatze bat baliatuz pribilegioak lituzkeen erasotzaile lokal batek pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2019-14611 identifikatzailea erreserbatu da.
    - Mugez kanpoko idazketa bat baliatuz pribilegioak lituzkeen erasotzaile lokal batek pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2019-14612 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

SAPen 2019ko abenduko segurtasun eguneraketa

Argitalpen data: 2019/12/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa;
- SAP Adaptive Server Enterprise, 15.7 eta 16.0 bertsioak;
- SAP BusinessObjects Business Intelligence Platform (Fiori BI Launchpad), 4.2 bertsioa;
- SAP ERP HCM (SAP_HRCES), 3. bertsioa;
- SAP Enable Now, 1911 bertsioa;
- SAP Portfolio and Project Management, S4CORE 102, 103, EPPM 100, CPRXRPM 500_702, 600_740 eta 610_740 bertsioak;
- SAP BusinessObjects Business Intelligence Platform (Monitoring Application), 4.1, 4.2 eta 4.3 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 6 segurtasun ohar eta eguneraketa bat argitaratu ditu. Horietatik 1 larritasun kritikokoa da eta 6 larritasun ertainekoak.

Argitaratutako ahultasun motak honako hauek dira:

- baimenaren egiaztapen gabeziako ahultasun bat;
- informazio zabalkunde erako 4 ahultasun;
- CSRF (Cross-Site Request Forgery) erako ahultasun bat;
- XSS (Cross-Site Scripting) erako ahultasun bat;
- beste era batzuetako 2 ahultasun.

Segurtasun ohartarazpen nagusia honi buruzkoa da:

- SAPek SAP Business Client-erako Google Chromium-en bertsio bateragarriaren eguneraketa argitaratu du, baina zerbitzua duen bertsioak oraindik ez ditu konpontzen Googlek argitaratutako CVE-2019-13720 eta CVE-2019-13721 ahultasunak. Gainera, CVE-2019-13720 ahultasuna baliatuko balitz, SAP sistemak zeharka kaltetuak izan litezke sare berera konektatutako ekipo bezero kutsatuen bidez. Hurrengo eguneraketak horren eraginak arindu litzake.

Gainerako ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2019-0402, CVE-2019-0395, CVE-2019-0405, CVE-2019-0403, CVE-2019-0404, CVE-2019-0399 eta CVE-2019-0398.CVE-2019-0325 identifikatzailea erreserbatu egin da.

Etiketak: Eguneraketa, SAP, Ahultasuna

Ahultasuna IBMren Spectrum Scale-n

Argitalpen data: 2019/12/11

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Spectrum Scale, 5.0.0.0 - 5.0.4.0 eta 4.2.0.0 - 4.2.3.18 bertsioak.

Azalpena:

IBMk segurtasun ahultasun bat aurkitu du IBM Spectrum Scale-n. Hori baliatuz autentifikatutako urruneko erasotzaile batek sisteman komando arbitrarioak exekuta litzake.

Konponbidea:

Eguneraketak 5.0.4.1 edo 4.2.3.19 bertsioetara ezartzea.

Xehetasuna:

Bereziki diseinatutako eskaera bat bidaliz, erasotzaile batek komando arbitrarioak exekuta litzake sisteman. Ahultasun horretarako CVE-2019-4715 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Microsoften 2019ko abenduko segurtasun buletina

Argitalpen data: 2019/12/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows,
- Internet Explorer,
- Microsoft Office, Microsoft Office Services eta Web Apps,
- SQL Server,
- Visual Studio,
- Skype for Business.

Azalpena:

Segurtasun eguneraketei buruzko Microsoften azaroko argitalpenean 35 ahultasun jaso dira, horietatik 7 kritiko gisa sailkatu dira eta 28 garrantzitsu gisa.

Konponbidea:

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

Xehetasuna:

Argitaratutako ahultasun motak honako hauek dira:

- informazioaren zabalkundea,
- pribilegioen eskalatzea,
- zerbitzuaren ukapena,
- kodearen urruneko exekuzioa,
- segurtasun ezaugarria saihestea,
- identitatea ordeztea.

Etiketak: Eguneraketa, Microsoft, Windows

Hainbat ahultasun Xen-en

Argitalpen data: 2019/12/12

Garrantzia: Altua

Kaltetutako baliabideak:

- Xen-en bertsio guztiak.
- Citrix Hypervisor 8.0 eta lehenagokoak.
- Citrix XenServer 7.6.
- Citrix XenServer 7.1 LTSR CU2.
- Citrix XenServer 7.0.

Azalpena:

Xen-ek bere produktuei eragiten dieten zazpi ahultasun aurkitu ditu. Urruneko erasotzaile batek ustekabeko itxiera eragin lezake, zerbitzuaren ukapen egoera (DoS) eragin, pribilegioak eskalatu edo informazioa hedatu.

Konponbidea:

Xen-ek eguneraketa multzo bat argitaratu du ahultasunak arintzeko.

Informazio gehiago eskuratzeko Erreferentziak atala irakurri.

Xehetasuna:

Aurkitutako ahultasunak baliatuz urruneko erasotzaile batek honakoa egin lezake:

- Ustekabeko itxiera,
- zerbitzuaren ukapen egoera (DoS) eragitea,
- pribilegioak eskalatzea,
- informazioa zabaltzea.

Ahultasun horietarako CVE-2019-14607, CVE-2019-19577, CVE-2019-19578, CVE-2019-19580, CVE-2019-19581, CVE-2019-19582 eta CVE-2019-19583 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Ahultasuna

WordPress-entzat 5.3.1 segurtasun eguneraketa

Argitalpen data: 2019/12/13

Garrantzia: Altua

Kaltetutako baliabideak:

WordPress, 5.3 eta lehenagoko bertsioak.

Azalpena:

Segurtasun eta mantenu bertsio honek 46 zuzenketa eta hobekuntza ditu. Gainera hainbat segurtasun zuzenketa ere jasotzen ditu.

Konponbidea:

Ahultasun horiek konpontzeko WordPress edukien kudeatzailearen 5.3.1 bertsioa argitaratu da, eta haien deskargen orrian eskuragarri dago.

Xehetasuna:

Segurtasun zuzenketek honako ahultasun hauek konpontzen dituzte:

- Pribilegiorik gabeko erabiltzaile batek mezu bat bidal lezake API RESTen bidez.
- *Cross-site scripting* (XSS), ondo sortutako esteketan gorde litekeena.
- *hardening en wp_kses_bad_protocol*() egin liteke "bi puntuak" atributua ezagutzen duela ziurtatzeko.
- XSS iraunkorra, blokeen editorearen edukia erabiliz.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun Dell EMCren XtremIO-n

Argitalen data: 2019/12/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Dell EMC XtremIO X2 XMS, 6.3.0 bertsioa baino lehenagokoak.

Azalpena:

Lukasz Plonka-k hiru ahultasun aurkitu ditu Dell EMCren XtremIO produktuan, bat larritasun kritikokoa eta besteak larritasun ertainekoak. Ahultasun horiek baliatuz urruneko erasotzaile batek arriskuan jar lezake kaltetutako sistema.

Konponbidea:

Dell EMC XtremIO XMS 6.3.0 bertsiora edo berriagora eguneratzea.

Xehetasuna:

- Larritasun kritikoko ahultasuna baliatuz, urruneko sarbidea lukeen eta ahultasuna baliatzeko pribilegioen maila baxua lukeen erasotzaile batek biltegiratutako XSS (*Cross-Site Scripting*) erako eraso bat egin lezake, eta aplikazioaren eremuetan asmo gaiztoko HTML edo JavaScript kodea gorde lezake. Erabiltzaileak beren nabigatzaileen bitartez orrialde injektatura sartzen direnean, web nabigatzaileak asmo gaiztoko kodea exekuta dezake web aplikazio ahularen testuinguruan. Ahultasun horretarako CVE-2019-18578 identifikatzailea erreserbatu da.
- Larritasun ertaineko ahultasunak honakoak dira:
  - Informazioren hedapen erako ahultasun bat aurkitu da, sistema eragileko erabiltzaileen pasahitzak fitxategi lokaletan gordetzen dituena. Erregistroko fitxategietara sarbidea lukeen erasotzaile lokal batek agerian utzitako pasahitzak erabil litzake XtremIOra sartzeko, kaltetutako erabiltzailearen pribilegioekin. Ahultasun horretarako CVE-2019-18576 identifikatzailea erreserbatu da.
  - Baimenen esleitze oker erako ahultasun bat baliatzea lortuz gero, XtremIO-n *xinstall* pribilegioak lituzkeen erasotzaile lokal batek root-era sarbidea lor lezake. Ahultasun horretarako CVE-2019-18577 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Joomla! 3.9.14ren segurtasun eguneraketa

Argitalpen data: 2019/12/18

Garrantzia: Txikia

Kaltetutako baliabideak:

Joomla! CMS, 2.5.0tik 3.9.13ra bitarteko bertsioak.

Azalpena:

Joomla!-k bertsio berri bat argitaratu du, bere nukleoak dituen kritikotasun txikiko bi ahultasun konpontzen dituena, bidearen ezagutarazte eta SQL injekzio erakoak.

Konponbidea:

3.9.14 bertsiora eguneratzea.

Xehetasuna:

- Sarbidearen egiaztatze falta erako ahultasun bat aurkitu da *framework*-aren fitxategietan. Hori baliatuz horiek kokatzen diren bidea ezagutzera eman liteke. Ahultasun horretarako CVE-2019-19845 identifikatzailea erabili da.
- SQL kontsultetan erabiltzen diren konfigurazio parametroek duten egiaztatze falta baliatuz, SQL injekzio erako erasoak egin litezke. Ahultasun horretarako CVE-2019-19846 identifikatzailea erabili da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Ahultasuna Citrix Application Delivery Controller eta Citrix Gateway-en

Argitalpen data: 2019/12/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Citrix ADC eta Citrix Gateway, 13.0 bertsioa, zerbitzua duten build guztiak;
- Citrix ADC eta NetScaler Gateway, 12.1 bertsioa, zerbitzua duten build guztiak;
- Citrix ADC eta NetScaler Gateway, 12.0 bertsioa, zerbitzua duten build guztiak;
- Citrix ADC eta NetScaler Gateway, 11.1 bertsioa, zerbitzua duten build guztiak;
- Citrix NetScaler ADC eta NetScaler Gateway, 10.5 bertsioa, zerbitzua duten build guztiak.

Azalpena:

Ahultasun bat aurkitu da Citrix produktuetan. Hori baliatuz erasotzaile batek kodea arbitrarioki exekuta lezake.

Konponbidea:

Citrix-ek laster eguneraketa bat argitaratuko du. Bitartean posible da ondoko dokumentuan azaltzen diren arintze neurriak ezartzea: CVE-2019-19781rako arintze urratsak.

Xehetasuna:

Citrix Application Delivery Controller (ADC) eta Citrix Gateway-k duten ahultasun bat baliatuz, autentifikatu gabeko erasotzaile batek kodea arbitrarioki exekuta lezake. Ahultasun horretarako CVE-2019-19781 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna TP-Link-en Archer routerretan

Argitalpen data: 2019/12/18

Garrantzia: Altua

Kaltetutako baliabideak:

- Archer C5 V4,
- Archer MR200v4,
- Archer MR6400v4,
- Archer MR400v3.

Azalpena:

TP-Link-ek kritikotasun altuko ahultasun bat aurkitu du bere Archer gamaren gailu batzuei eragiten diena. Urruneko erasotzaile batek autentifikazioa saihets lezake eta gailuaren kontrola hartu.

Konponbidea:

TP-Link-ek kaltetutako produktuetan ahultasuna konpontzen duten eguneraketak argitaratu ditu.

- Archer C5 V4,
- Archer MR200v4,
- Archer MR6400v4,
- Archer MR400v3.

Xehetasuna:

Ahultasuna gertatzen da bereziki diseinatutako HTTP pakete bat bidaltzean, routerrak beti onartzen baitu, eta horrela gailuan aldaketak egin daitezke. Urruneko erasotzaile batek ahultasun hori balia lezake gailuaren kontrola hartzeko administratzaile baimenekin (root). Ahultasun horretarako CVE-2019-7405 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Ahultasuna IBMren Planning Analytics-en

Argitalpen data: 2019/12/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

IBM Planning Analytics, 2.0.0tik 2.0.8ra bitarteko bertsioak.

Azalpena:

IBMk konfigurazioaren gainidazketa erako ahultasun baten berri eman du. Hori baliatuz, erasotzaile batek administratzaile modura sarbidea lor lezake.

Konponbidea:

Ahultasun hori konpontzeko IBM-k 2.0.9 bertsioa argitaratu du.

Xehetasuna:

IBM Planning Analytics ahula da konfigurazioaren gainidazketa baten aurrean. Hori baliatuz autentifikatu gabeko erasotzaile batek "admin" modura saioa has lezake eta, jarraian, *root* edo SYSTEM modura kodea exekutatu, TM1 komandoen sekuentzia baten bidez.Ahultasun horretarako CVE-2019-4716 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun TIBCO produktuetan

Argitalpen data: 2019/12/18

Garrantzia: Altua

Kaltetutako baliabideak:

- TIBCO Spotfire Analyst, honako bertsioak:
  - 7.11.1 eta lehenagokoak;
  - 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, 10.3.2, 10.4.0, 10.5.0 eta 10.6.0.
- TIBCO Spotfire Analytics Platform para AWS Marketplace, 10.6.0 bertsioa;
- TIBCO Spotfire Deployment Kit, 7.11.1 eta lehenagoko bertsioak;
- TIBCO Spotfire Desktop, honako bertsioak:
  - 7.11.1 eta lehenagokoak;
  - 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, 10.3.2, 10.4.0, 10.5.0 eta 10.6.0.
- TIBCO Spotfire Desktop Language Packs,7.11.1 eta lehenagoko bertsioak;
- TIBCO Spotfire Server, honako bertsioak:
  - 7.11.7 eta lehenagoko bertsioak;
  - 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.4.0, 10.5.0 eta 10.6.0.
- Osagaiak:
  - bistaratzeak;
  - datuetarako sarbide geruza;
  - Spotfire liburutegia.

Azalpena:

TIBCOk larritasun altuko hiru ahultasun aurkitu ditu. Autentifikatu gabeko urruneko erasotzaile batek kodea exekuta lezake, partekatutako datu iturrietarako kredentzialak agerian utzi edo XSS islatua eragin.

Konponbidea:

- TIBCO Spotfire Analyst eta TIBCO Spotfire Desktop:
  - 7.11.1 eta lehenagoko bertsioen kasuan, 7.11.2 edo goragokoetara eguneratzea;
  - 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1 eta 10.3.2 bertsioen kasuan, 10.3.3 edo goragokoetara eguneratzea;
  - 10.4.0, 10.5.0 eta 10.6.0 bertsioen kasuan, 10.6.1 edo goragokoetara eguneratzea.
- AWS Marketplace-rako TIBCO Spotfire Analytics Platform: 10.6.1 edo goragokoetara eguneratzea;
- TIBCO Spotfire Deployment Kit: 7.11.2 edo goragokoetara eguneratzea;
- TIBCO Spotfire Desktop Language Packs, 7.11.2 edo goragokoetara eguneratzea;
- TIBCO Spotfire Server:
-
  - 7.11.7 eta lehenagoko bertsioen kasuan, 7.11.8 edo goragokoetara eguneratzea;
  - 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3 eta 10.3.4 bertsioen kasuan, 10.3.5 edo goragokoetara eguneratzea;
  - 10.4.0, 10.5.0 eta 10.6.0 bertsioen kasuan, 10.6.1 edo goragokoetara eguneratzea.

Xehetasuna:

- Aurkitu den ahultasun bat baliatuz, pribilegioak lituzkeen erasotzaile batek DXP fitxategiak alda litzake *Spotfir*e liburutegian, eta horrela urrunetik kodea exekuta lezake sistemara sarbidea duten beste erabiltzaile batzuen kontuan. Ahultasun horretarako CVE-2019-17334 identifikatzailea erabili da.
- Erasotzaile batek *Spotfire*-ren datuen iturrietara sartzeko erabiltzen diren kredentzialak eskuratzeko beharrezkoa den informaziora sarbidea lor lezake. Ahultasun hau soilik balia daiteke NTLM edo profil baten kredentzialak erabiltzen ari direnean. Ahultasun horretarako CVE-2019-17336 identifikatzailea erabili da.
- XSS islatu erako ahultasun bat baliatuz erasotzaile batek administratzaile sarbide osoa lor lezake kaltetutako produktuen web interfazera. Ahultasun horretarako CVE-2019-17337 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Kodearen urruneko exekuzioa Microsoft Windows-ek erabiltzen duen WebDAV protokoloan

Argitalpen data: 2019/12/19

Garrantzia: Altua

Kaltetutako baliabideak:

WebDAV protokoloa erabiltzen duten Microsoft Windows-en bezeroak.

Azalpena:

Ahultasun hau baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta dezake Microsoft Windows-en kaltetutako ekipoetan.

Konponbidea:

Ahultasunaren izaera kontuan izanik, arintze estrategia nabarmen bakarra zerbitzuarekiko interakzioa konfiantzako makinek soilik izatea da.

Xehetasuna:

Akats zehatza WebDAV bideen erabilpenean datza. HTTP protokoloaren luzapen batek bezeroei ahalbidetzen die urruneko operazioak egitea web edukia sortzeko. Bereziki diseinatutako WebDAV bide batek sistemaren dei baten exekuzioa eragin dezake erabiltzaileak eskainitako kate batez osatutakoa. Urruneko erasotzaile batek ahultasun hau balia lezake kodea exekutatzeko uneko erabiltzailearen testuinguruan.

Etiketak: 0day, Ahultasuna

Hainbat ahultasun Drupal-en core-an

Argitalpen data: 2019/12/19

Garrantzia: Altua

Kaltetutako baliabideak:

- 7.x,
- 8.8.x,
- 8.7.x

Azalpena:

Drupal-en segurtasun ekipoak hainbat ahultasun aurkitu ditu core-an. Horiek baliatuz, erasotzaile batek zerbitzuaren ukapen egoera eragin lezake, *.htaccess* fitxategiaren babesak saihestu, edo babestutako multimedia elementuetara sarbidea lortu, besteak beste.

Konponbidea:

7.69, 8.8.1 eta 8.7.11 bertsioetara eguneratzea.

Xehetasuna:

- Larritasun altuko hainbat ahultasun daude Drupal konfiguratuta dagoenean .tar, .tar.gz, .bz2 edo .tlz fitxategiak kargatzeko eta prozesatzeko. Horien jatorria da hirugarrenen *Archive_Tar* liburutegiak duen ahultasun bat.
- Multimedia liburutegiaren moduluak ez du aski murrizten multimedia elementuetarako sarbidea zenbait konfiguraziotan.
- Drupal 8ren nukleoaren *file_save_upload()* funtzioak ez du ezabatzen hasierako eta amaierako puntua ('.') fitxategien izenetatik. Ekarpen modura gehitutako moduluekin edozein luzapeneko fitxategiak igotzeko gaitasuna duten erabiltzaileek ahultasun hau balia dezakete .htaccess bezalako sistema fitxategiak igotzeko, horrela saihestuz Drupal-en *.htaccess* lehenetsitako fitxategiak eskaintzen dituen babesak.
- *install.php* fitxategira sartzeak eragin dezake cacheko datuak hondatzea eta ataria eraginda gelditzea horiek berreraiki bitartean.

Etiketak: Eguneraketa, CMS, Ahultasuna

XSS erako ahultasuna Dell EMCren PowerMax-erako Unisphere-n

Argitalpen data: 2019/12/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

PowerMax-erako Dell EMC Unisphere, 9.1.0.9 baino lehenagoko bertsioak.

Azalpena:

Tomasz Stachowicz ikertzaileak, Dell EMCrekin lankidetzan, larritasun kritikoko ahultasun bat aurkitu du. Autentifikatutako urruneko erasotzaile batek kode arbitrarioa exekuta lezake sisteman.

Konponbidea:

PowerMax-erako Dell EMC Unsiphere 9.1.0.9 edo bertsio berriagoetara eguneratzea.

Xehetasuna:

Softwareak duen *Cross-site-scripting* (XSS) erako ahultasun bat baliatuz, urruneko erasotzaile autentifikatu batek JavaScript kodea injekta lezake sisteman eta erabiltzailearen beste saio batzuei eragin. Ahultasun horretarako CVE-2019-18588 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Murrizpen desegoki erako ahultasuna Palo Alto PAN-OSen

Argitalpen data: 2019/12/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

PAN-OS 9.0, 9.0.5-h3 baino lehenagoko bertsioak PA-7000 Series-en, bigarren belaunaldiko SMCrekin (*Switch Management Card*) eta LFC (*Log Forwarding Card*) instalatuta eta konfiguratuta.

Azalpena:

KAUSTeko Ayad (Ed) Sleiman-ek eta bere ekipoak LFCrako komunikazioek duten murrizpen desegoki erako ahultasun bat aurkitu eta ezagutzera eman dute.

Konponbidea:

9.0.5-h3 eta geroagoko bertsioek eta 8218-5815 eduki eguneraketak ahultasun hori konpontzen dute.

Xehetasuna:

Aurreikusitako *endpoint*-etan komunikazio kanalaren murrizpen desegoki erako ahultasun bat baliatuz, LFCren sarera sarbidea lukeen erasotzaile batek sarbidea lor lezake *root* pribilegioekin PAN-OSera. Ahultasun horretarako CVE-2019-17440 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun IBMren Watson Studio Local-en

Argitalpen data: 2019/12/23

Garrantzia: Altua

Kaltetutako baliabideak:

- IBM Watson Studio Local, 1.2.3 bertsioa.

Azalpena:

Watson Studio Local-ek dituen larritasun altuko hainbat ahultasunen berri eman du IBMk.

Konponbidea:

Honako eguneraketa aplikatzea.

Xehetasuna:

- Esteka sinbolikoekin zerikusia zuen ahultasun bat baliatuz, Watson Studio Local-en erabiltzaileen direktoriora sarbide arbitrarioa lor zitekeen.
- Sarrera datuen baliozkotze faltak eraso aukera bat eskaintzen du APIrako hainbat deietan.
- Lehenagoko SSL protokoloaren zerbitzua bertan behera utzi zen.

Etiketak: Eguneraketa, IBM, Ahultasuna

Memoria ihesa tmrouted prozesuan F5en BIG-IP-n

Argitalpen data: 2019/12/26

Garrantzia: Altua

Kaltetutako baliabideak:

- BIG-IP (LTM), honako bertsioak:
  - 15.0.0 - 15.0.1;
  - 14.1.0 - 14.1.2;
  - 14.0.0 - 14.0.1;
  - 13.1.0 - 13.1.3;
  - 12.1.0 - 12.1.5.

Azalpena:

Routing lizentzia duten eta Multicast Forwarding Cache-rekin (MFC) konfiguratuta dauden BIG-IP sistemek duten ahultasun bat baliatuz, erasotzaile batek zerbitzuaren ukapena eragin lezake.

Konponbidea:

Honako bertsioetara eguneratzea:

- 15.1.0,
- 14.1.2.1,
- 14.0.1.1,
- 13.1.3.2.

Xehetasuna:

Routing lizentzia duen eta Multicast Forwarding Cache-rekin (MFC) konfiguratuta dagoen BIG-IP sistema batek tmrouted prozesuan memoriaren ihesa jasan lezake, sistemaren baliabideak agortu, eta hori berrabiarazi. Hori baliatuz erasotzaile batek zerbitzuaren ukapena eragin lezake. Ahultasun horretarako CVE-2019-6681 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Parametroen injekzio erako ahultasuna IBM Spectrum Scale-n

Argitalpen data: 2019/12/26

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Elastic Storage Server, honako bertsioak:

- 5.3.0 bertsiotik 5.3.4.1 bertsiora bitartean;
- 5.0.0 bertsiotik 5.2.7.0 bertsiora bitartean;
- 4.5.0 bertsiotik 4.6.0.0 bertsiora bitartean;
- 4.0.0 bertsiotik 4.0.6.0 bertsiora bitartean.

Azalpena:

IBM Elastic Storage Server-i IBM Spectrum Scale-k duen ahultasun batek eragiten dio. Horren bitartez, root pribilegioak eskura daitezke setuid fitxategietan parametroak injektatuz.

Konponbidea:

- IBM Elastic Storage Server-en kasuan, 5.0.0 bertsiotik 5.3.4.1 bertsiora bitartekoak, 5.3.4.2 bertsiora eguneratzea;
- IBM Elastic Storage Server-en kasuan, 5.0.0 bertsiotik 5.2.7.0 bertsiora bitartekoak, 5.2.8 bertsiora eguneratzea;
- Ez bada posible IBM Elastic Storage Server-en 5.3.2.0 edo 5.2.5 bertsioetara eguneratzea, IBM Service-rekin harremanetan jarri efix bat eskuratzeko:
  - IBM Elastic Storage Server-en kasuan, 5.3.0.0 bertsiotik 5.3.4.1 bertsiora bitartekoak, APAR IJ18477 ezarri;
  - IBM Elastic Storage Server-en kasuan, 5.0.0.0 bertsiotik 5.2.7.0 bertsiora bitartekoak, APAR IJ18518 ezarri;
  - IBM Elastic Storage Server-en kasuan, 4.0.0 bertsiotik 4.6.0 bertsiora bitartekoak, APAR IJ18518 ezarri.

Xehetasuna:

Ahultasun bat aurkitu da IBM Spectrum Scale-ren maila guztietan, 5.0.0.0tik 5.0.3.2ra bitarteko bertsioak eta 4.2.0.0tik 4.2.3.17ra bitarteko bertsioak. Hori baliatuz, erasotzaile batek root pribilegioak eskura litzake setuid fitxategietan parametroak injektatuz. Ahultasun horretarako CVE-2019-4558 identifikatzailea erabili da.

Etiketak: Eguneraketa, IBM, Ahultasuna