2019ko Apirilaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun IBMren Security Privileged Identity Manager Appliance-n

Argitalpen data: 2019/04/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IBM Security Privileged Identity Manager, 2.1.1 bertsioa

Azalpena:

IBMk segurtasun buletin bat argitaratu du. Guztira 48 ahultasun agertzen dira, bat larritasun kritikokoa, 16 larritasun altukoak eta gainerakoak ertain edo baxukoak.

Konponbidea:

IBMk ahultasun horiek arintzen dituen partxe bat argitaratu du, lotura honetatik deskarga daitekeena.

Xehetasuna:

Aurkitutako ahultasunak era honetakoak dira:

- Pribilegioen eskalatzea.
- Ustekabeko itxiera.
- Komandoen exekuzio arbitrarioa.
- Kodearen exekuzio arbitrarioa.
- Memoriaren akatsa.
- Zerbitzuaren ukapen egoera eragitea.
- Informazioa ezagutaraztea
- Sarbide murrizpenak saihestea.
- Cookieak aldatzea edota injektatzea.

Larritasun kritikoko ahultasunari CVE-2017-16939 identifikatzailea esleitu zaio. Larritasun altukoei ondoko identifikatzaileak esleitu zaizkie: CVE-2018-1087, CVE-2018-1068, CVE-2016-1181, CVE-2014-0114, CVE-2018-15688, CVE-2018-5391, CVE-2017-1000050, CVE-2018-0494, CVE-2018-1113, CVE-2018-8897, CVE-2015-5180, CVE-2017-15670, CVE-2017-18017 eta CVE-2017-11368. Eta kritikotasun altuko ahultasunetarako ondoko identifikatzaileak erreserbatu dira: CVE-2018-1640 eta CVE-2018-1618.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Apache HTTP Server-en

Argitalpen data: 2019/04/02

Garrantzia: Handia

Kaltetutako baliabideak:

- Apache HTTP Server, honako bertsioak: 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1 eta 2.4.0.

Azalpena:

Apachek 6 ahultasunen berri eman du, 3 larritasun altukoak eta beste 3 larritasun baxukoak.

Konponbidea:

- 2.4.39 bertsiora eguneratzea.

Xehetasuna:

Kritikotasun altuko ahultasunak ondokoak dira:

- Pribilegio gutxiko bigarren mailako prozesu edo azpi-prozesuetan event, worker edo prefork MPM (*Prozesatze Anitzeko Moduluak*) duen Apache HTTP Server-en exekutatzen den kodeak (script-en interpretatzaile batek exekutatutako *script*-ak barne) erasotzaile bati ahalbidetu liezaioke kode arbitrarioa exekutatzea root pribilegioekin markagailua manipulatuz. Ahultasun horretarako CVE-2019-0221 identifikatzailea erreserbatu da.
- Azpi-prozesuen zerbitzari batean exekutatzen ari denean *mod_auth_digest*-ek duen sekuentzia baldintza batek kredentzial baliogarriak dituen erasotzaile bati ahalbidetu liezaioke autentifikazioa egitea beste erabiltzaile izen bat erabiliz eta sarbide kontroleko murrizpenak saihestuz. Ahultasun horretarako CVE-2019-0217 identifikatzailea erreserbatu da.
- TLSv1.3rekin kokapenaren araberako bezeroaren ziurtagirien egiaztapena erabiltzean *mod_ssl*-ek duen akats batek *Post-Handshake* autentifikazioa onartzen duen erasotzaile bati ahalbidetu liezaioke sarbide kontrolaren murrizpenak saihestea. Ahultasun horretarako CVE-2019-0215 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako ondoko identifikatzaileak erreserbatu dira: CVE-2019-0197, CVE-2019-0196 eta CVE-2019-0220.

Etiketak: Eguneraketa, Apache, Ahultasuna.

Hainbat ahultasun IBMren Db2-n

Argitalpen data: 2019/04/03

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM Db2, V9.7, V10.1, V10.5 eta V11.1, plataforma guztietan.

Azalpena:

Db2-k dituen buffer overflow erako bi ahultasunen berri eman da. Horiek baliatuz erasotzaile lokal batek kode arbitrarioa exekuta lezake root modura.

Konponbidea:

- Partxe egokia aplikatzea bertsioaren arabera. Erreferentziak kontsultatzea.

Xehetasuna:

- IBM DB2 libdb2e.so.1-ek pila batean oinarritutako bufferraren gainezkatzearen ahultasuna dauka, mugen egiaztatze oker batek eraginda. Hori baliatuz erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2018-1936 identifikatzailea erreserbatu da.
- Linux, UNIX eta Windows-erako IBM DB2 (DB2 Connect Server barne) ahula da bufferraren gainezkatzearen aurrean. Hori baliatuz autentifikatutako erasotzaile lokal batek kode arbitrarioa exekuta lezake sisteman root modura. Ahultasun horretarako CVE-2019-4014 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Ahultasuna FortiOS-en

Argitalpen data: 2019/04/05

Garrantzia: Handia

Kaltetutako baliabideak:

- FortiOS, honako bertsioak:
  - 6.0.2 eta lehenagokoak.
  - 5.6.7 eta lehenagokoak.
  - 5.4.10 eta lehenagokoak.

Azalpena:

Autentifikatutako eta pribilegiorik gabeko erabiltzaile batek birbideratzearen konfigurazioa alda lezake.

Konponbidea:

Kaltetutako produktuaren arabera, honako bertsioetara eguneratzea:

- 6.0.3 edo goragokoa.
- 5.6.8 edo goragokoa.
- 5.4.11 edo goragokoa.

Xehetasuna:

- FortiOS-en sistemaren ahultasunaren kanpo kontrol batek erabiltzaile autentifikatu bati ahalbidetu liezaioke gailuaren birbideratzearen hobespenak aldatzea ZebOS osagairako konexioaren bidez. Ahultasun horretarako CVE-2018-13371 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioen eskalatzea Synergy-rako 16 Gb HPE Virtual Connect SEren Fibre Channel Moduluan

Argitalpen data: 2019/04/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Synergy-rako 16 Gb HPE Virtual Connect SEren Fibre Channel Moduluak duen ahultasun batek baimenik gabeko pribilegioen eskalatzea ahalbidetu dezake modu lokalean edo urrunetik.

Azalpena:

Una vulnerabilidad en el módulo Fibre Channel de 16 Gb HPE Virtual Connect SE para Synergy podría permitir la elevación no autorizada de privilegios local o remota.

Konponbidea:

- HPE Synergy Custom SPP 2018.11.20190405 eta HPE Synergy Custom SPP 2019.03.20190401 bertsio eguneratuetan dagoen firmware -aren 5.51.01 bertsiora eguneratzea, biak eskuragarri deskarga orrialde honetan: HPE Synergy Software Release

Xehetasuna:

- Ahultasuna baliatuz pribilegioak igo litezke baimenik gabe modu lokalean edo urrunetik. Ahultasun horretarako CVE-2018-7120 identifikatzailea erreserbatu da.

Etiketak: HP, Ahultasuna

Hainbat ahultasun IBMren produktuetan

Argitalpen data: 2019/04/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IBM QRadar SIEM 7.3.2 GA - 7.3.2 GA Interim Fix 1
- IBM API Connect, 2018.1-2018.4.1.3 bertsioa

Azalpena:

IBMk bere bi produktuk dituzten ahultasunen berri eman du. Horietakoren bat arrakastaz baliatuz gero, autentifikazioa saihets liteke edo pribilegioak eskalatzea lortu.

Konponbidea:

- IBM QRadar SIEMen kasuan, 7.3.2 GA - 7.3.2 GA Interim Fix 2 bertsiora eguneratzea
- IBM API Connect-en kasuan, 2018.4.1.4 fixpack bertsiora eguneratzea

Xehetasuna:

- IBM QRadar SIEM-ek duen ahultasun bat baliatuz, erasotzaile batek autentifikazioa saihets lezake, funtzionaltasunen bat agerian jarriz. Ondorioz informazioaren hedapena gerta liteke edo aplikazioaren konfigurazioaren aldaketa. Ahultasun horretarako CVE-2019-4210 identifikatzailea erreserbatu da.
- IBM API Connect's Developer Portal-ek duen ahultasun bat baliatuz, erasotzaile batek pribilegioen eskalatzea lor lezake OpenID Connect-en (OIDC) erabiltzaile erregistro batekin integratzen denean. Ahultasun horretarako CVE-2019-4155 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Microsoften 2019ko apirileko segurtasun buletina

Argitalpen data: 2019/04/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows
- Microsoft Edge
- Internet Explorer
- Azure
- Microsoft Exchange
- Team Foundation Server
- Open Enclave SDK
- ASP .NET

Azalpena:

Segurtasun eguneraketei buruzko Microsoften hileroko argitalpenean 75 ahultasun jaso dira oraingoan, 16 kritiko gisa sailkatu dira eta 59 garrantzitsu gisa.

Konponbidea:

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

Xehetasuna:

Argitaratutako ahultasun motak ondokoak dira:

- pribilegioen eskalatzea,
- informazioa zabaltzea,
- kodearen urruneko exekuzioa,
- manipulazioa,
- ordezpena,
- zerbitzuaren ukapena.

Etiketak: Eguneraketa, Microsoft, Nabigatzailea, Ahultasuna, Windows

---

Ahultasuna TIBCOren ActiveMatrix BusinessWorks-en autentifikazioan

Argitalpen data: 2019/04/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- TIBCO ActiveMatrix BusinessWorks, 6.4.2 eta lehenagoko bertsioak.

Azalpena:

BusinessWork-en HTTP Connector osagaiak ahultasun bat dauka. Hori baliatuz asmo gaiztoko HTTP bezero batek arrakastaz exekuta litzake HTTP eskariak autentifikatu gabe, XMLrekin autentifikazio oinarrizkoa erabiltzen denean.

Konponbidea:

- 6.5.0 edo goragoko bertsioetara eguneratzea.

Xehetasuna:

- HTTP Connector osagaiak duen ahultasun batek ahalbidetu egiten du BusinessWorks-ek autentifikaziorik gabeko HTTP erabiltzaileen eskariak prozesatzea, baita autentifikazioa behar denean ere. Hau soilik gerta daiteke HTTPren oinarrizko autentifikazio politika XMLrekin batera erabiltzen denean. BusinessWorks-ek lehenagoko HTTP eskari baten kredentzialak erabil litzake baimena lortzeko. Ahultasun horretarako CVE-2019-8990 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Pribilegioak eskalatzearen erako ahultasuna Intel-en Media SDK-n

Argitalpen data: 2019/04/10

Garrantzia: Handia

Kaltetutako baliabideak:

- Intel® Media SDK, 2018 R2.1 baino lehenagoko bertsioak

Azalpena:

Intel-ek ahultasun bat aurkitu du bere Intel® Media SDK produktuan, pribilegioen eskalatzea ahalbidetu lezakeena.

Konponbidea:

- Intelek gomendatzen du kaltetutako produktua 2018 R2.1 edo goragoko bertsiora eguneratzea bere deskargen zentrotik.

Xehetasuna:

- Intel(R) Media SDK produktuaren instalatzailean, 2018 R2.1 baino lehenagoko bertsioetan, direktorio baimen okerrak erabiltzen direla baliatuz, autentifikatutako erabiltzaile batek pribilegioen eskalatzea gaitu lezake sarbide lokalaren bidez. Ahultasun horretarako CVE-2018-18094 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Joomla! 3.9.5en segurtasun eguneraketa

Argitalpen data: 2019/04/10

Garrantzia: Handia

Kaltetutako baliabideak:

- Joomla! CMS, 1.5.0tik 3.9.4ra bitarteko bertsioak

Azalpena:

Joomla!-k bertsio berri bat argitaratu du, nukleoak dituen hiru ahultasun konpontzen dituena, bat kritikotasun altukoa, beste bat kritikotasun ertainekoa eta beste bat kritikotasun txikikoa. Ahultasun horiek era hauetakoak dira: sarbidearen kontrola bortxatzea, Cross-site scripting (XSS) eta direktorio jauzia.

Konponbidea:

- 3.9.5 bertsiora eguneratzea.

Xehetasuna:

- Kritikotasun altuko ahultasuna sarbidearen kontrol zerrenden (ACL) urratze bati dagokio. Autentifikaziorik gabeko erasotzaile batek baimenik gabeko eskaerak egin litzake, com_users-en "refresh list of helpsites" endpoint-ean dagoen sarbidearen egiaztapenaren akats bat baliatuz. Ahultasun horretarako CVE-2019-10946 identifikatzailea erreserbatu da.
- Kritikotasun ertaineko ahultasunari ez zaio identifikatzailerik esleitu, oraindik iragartzeko dagoelako.
- Kritikotasun baxuko ahultasunerako CVE-2019-10945 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, CMS, Windows

SAPen 2019ko apirileko segurtasun eguneraketa

Argitalpen data: 2019/04/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa
- SAP Crystal Reports for Visual Studio, 2010 bertsioa
- AP NetWeaver (SLD Registration) eta ABAP Platform (SLD Registration), honako bertsioak: KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT; KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT; KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49; KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KERNEL 7.21etik 7.22ra bitartean, 7.45 eta 7.49
- SAP BASIS, 7.00tik 7.02ra bitarteko bertsioak, 7.10etik 7.30era bitartekoak, 7.31, 7.40 eta 7.50etik 7.53ra bitartekoak
- SAP NetWeaver Process Integration (Runtime Workbench eta Messaging System), 7.10etik 7.11ra bitarteko bertsioak, biak barne, 7.31, 7.40 eta 7.50
- SAP HANA, 1.0 eta 2.0 bertsioak
- AP Enterprise Financial Services, honako bertsioak: SAPSCORE 1.13, 1.14, 1.15; S4CORE 1.01, 1.02, 1.03; EA-FINSERV 1.10, 2.0, 5.0, 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0 eta Bank/CFM 4.63_20

Azalpena:

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

Konponbidea:

- SAPen zerbitzuaren 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 3 eguneraketa eman ditu ezagutzera. Horietatik 1 larritasun kritikokoa da, 2 larritasun altukoak eta beste 6 larritasun ertainekoak.

Argitaratutako ahultasun motak ondokoak dira:

- Baimenaren egiaztapen gabeziako 2 ahultasun.
- Informazio zabalkundeko 3 ahultasun.
- XML External Entity (XXE) erako 2 ahultasun.
- Beste era batzuetako 2 ahultasun.

Kritikotzat kalifikatutako segurtasun eguneraketa honi buruzkoa da:

- Sap Business Client-ek barnean duen Chromium nabigatzaileak hainbat ahultasun ditu eta SAPek konpondu egin ditu eguneraketa honetan.

Kritikotasun altuko segurtasun oharrak honi buruzkoak dira:

- SAP Crystal Reports-ek informazioa hedatzearen ahultasuna dauka. Hori baliatuz erasotzaile batek informazio gehigarria zabal lezake (sistemako datuak, arazketa informazioa eta abar), eta horrek sistema ezagutzen eta eraso berriak planifikatzen lagunduko lioke. Ahultasun horretarako CVE-2019-0285 identifikatzailea erreserbatu da.
- AP NetWeaver Java Application Server-ek ordezpen erako ahultasun bat dauka. Erasotzaile batek datu irakurtezinak erakuts liezazkioke erabiltzaileari, edo bidaltzailearen helbidea, orrialde batean erakutsitako datuak edo bestelako informazio garrantzitsua aldatu. Ahultasun horretarako CVE-2019-0283 identifikatzailea erreserbatu da.

Gainerako ahultasunen identifikatzaileak honakoak dira: CVE-2019-0265, CVE-2019-0279, CVE-2019-0282, CVE-2019-0284, CVE-2019-0278 eta CVE-2018-2484.

Etiketak: Eguneraketa, SAP, Ahultasuna

Hainbat ahultasun IBren BigFix Platform-en

Argitalpen data: 2019/04/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IBM BigFix Platform, desde la versión 9.5 hasta la 9.5.11

Azalpena:

IBMk segurtasun buletin bat argitaratu du BigFix-ek erabiltzen dituen OpenSSL, Query eta YUI liburutegiek dituzten hainbat ahultasun jasoz, eta baita ahultasun kritiko zehatz bat ere, sisteman baimenik gabeko kargak ahalbidetu litzakeena.

Konponbidea:

- 9.5.12 eguneraketa partxea aplikatzea.
- Lotutako eguneraketa Fixlet-a exekutatzea kontsolan.

Xehetasuna:

- IBM BigFix Platform-ek autentifikatutako erabiltzaile bati ahalbidetu liezaioke zerbitzarira fitxategi bat igotzea pribilegio altuekin. Honen ondorioz azpiko sisteman baimenik gabeko exekuzio bat gerta liteke. Ahultasun horretarako CVE-2019-4013 identifikatzailea erreserbatu da.
- Gainerako ahultasunak Simultaneous Multi-Threading (SMT) eta cross-site scripting (XSS) erakoak dira. Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2018-5407, CVE-2012-5883, CVE-2012-6708 eta CVE-2015-9251.

Etiketak: Eguneraketa, IBM, Ahultasuna

Kodearen urruneko exekuzioaren erako ahultasuna Apache Tomcat-en

Argitalpen data: 2019/04/11

Garrantzia: Handia

Kaltetutako baliabideak:

- Apache Tomcat Windows plataforman, honako bertsioak:
  - 7.0.0tik 7.0.93ra bitartekoak
  - 8.5.0tik 8.5.39ra bitartekoak
  - 9.0.0.M1etik 9.0.17ra bitartekoak

Azalpena:

Ahultasun hau kanpoko segurtasun ikertzaile batek aurkitu zuen. Ondoren, EU FOSSA-2 proiektuak babesten duen *bug bounty* programaren bidez izan zen informatua Apache Tomcat-en segurtasun ekipoa 2019ko martxoaren 3an, eta 2019ko apirilaren 10ean argitaratu zen.

Konponbidea:

- 7.0.94 edo goragoko bertsiora eguneratzea.
- 8.5.40 edo goragoko bertsiora eguneratzea.
- 9.0.18 edo goragoko bertsiora eguneratzea.

Xehetasuna:

- Servlet CGI ahula da kodearen urruneko exekuzioaren (RCE) aurrean Windowsen exekutatzen denean *enableCmdLineArguments* gaituta dagoela. Horren arrazoia da JREk akats bat duela komandoen lerroko argumentuak Windowsera pasatzeko moduan. Servlet CGI desgaituta dago modu lehenetsian. CGIren *enableCmdLineArguments* aukera desgaituta dago modu lehenetsian Tomcat 9.0.x-en. Ahultasun horretarako CVE-2019-0232 identifikatzailea erabili da.

Etiketak: Eguneraketa, Apache, Ahultasuna

Komandoen injekzio erako ahultasuna Citrix-en

Argitalpen data: 2019/04/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- NetScaler SD-WAN Center 9.x, bertsio guztiak
- NetScaler SD-WAN Center, 10.0.7 baino lehenagoko 10.0.x bertsio guztiak
- Citrix SD-WAN Center, 10.1.x bertsio guztiak
- Citrix SD-WAN Center, 10.2.1 baino lehenagoko 10.2.x bertsio guztiak

Azalpena:

Citrix-ek bere bi produkturi eragiten dien komandoen injekzio erako ahultasun baten berri eman du.

Konponbidea:

- NetScaler SD-WAN Center-en kasuan, 10.0.7 edo goragoko bertsiora eguneratzea.
- Centro Citrix SD-WAN, 10.2.1 edo goragoko bertsiora eguneratzea.

Xehetasuna:

- Ahultasun hau arrakastaz baliatuz gero, administrazio kontsolara sarbidea lukeen autentifikaziorik gabeko erasotzaile batek *host*-a arriskuan jar lezake. Ahultasun horretarako CVE-2019-10883 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun F5en BIG-IPn

Argitalpen data: 2019/04/11

Garrantzia: Handia

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), ondoko bertsioak:
-
    - 14.0.0 - 14.1.0.1
    - 13.0.0 - 13.1.1.3
    - 12.10 - 12.1.4
    - 11.6.1 - 11.6.3
    - 11.5.1 - 11.5.8

Azalpena:

F5ek hainbat ahultasunen berri eman du, era ezberdinetakoak: XSS, zerbitzuaren ukapena eta pasahitzak modu ez-seguruan gordetzea.

Konponbidea:

- Ondoko bertsioetara eguneratzea:
-
    - 14.1.0.2
    - 13.1.1.4
    - 12.1.4.1
    - 11.6.4
    - 11.5.9

Xehetasuna:

- Boostrap-eko tooltip eta popover data-template atributuek XSS erasoak ahalbidetzen dituzte. Larritasun altuko ahultasun horretarako CVE-2019-8331 identifikatzailea erabili da.
- BIG-IP sistema ahula da zerbitzuaren ukapen (DoS) motako eraso baten aurrean, URLen sailkapena APM modulua erabiliz egiten denean. Larritasun altuko ahultasun horretarako CVE-2019-6610 identifikatzailea erreserbatu da.
- iSeries plataformetan secureKeyCapable atributua ez dago ezarrita. Horren ondorioz Secure Vault funtzioak ez du F5 hardwarearekiko bateragarritasuna erabiltzen unitatearen gakoa gordetzeko. Ondorioz, unitatearen gakoa testu lauan gordetzen da. Larritasun ertaineko ahultasun honetarako CVE-2019-6609 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat ahultasun Juniper gailuetan

Argitalpen data: 2019/04/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Service Insight, 15.1R1etik aurrerako bertsioak eta 18.1R1 baino lehenagokoak
- Service Now-ren bertsioak, 15.1R1etik aurrerako bertsioak eta 18.1R1 baino lehenagokoak
- Juniper Identity Management Service, 1.1.4 baino lehenagoko bertsioak
- Junos OS:
-
    - 12.1X46, 12.1X46-D25 baino lehenagoko bertsioak, bera barne, eta SRX seriean 12.1X46-D71, 12.1X46-D73 eta 12.1X46-D77 baino lehenagoko bertsioak
    - 12.1X46, 12.1X46-D82 baino lehenagoko bertsioak SRX5000 seriean
    - 12.3, 12.3R12-S10 baino lehenagoko bertsioak
    - 12.3X48, 12.3X48-D50 eta 12.3X48-D75 baino lehenagoko bertsioak SRX seriean
    - 12.3X48, 12.3X48-D80 baino lehenagoko bertsioak SRX5000 seriean
    - 14.1X53, serie hauetan: QFX5000, EX4300, EX4600
    - 14.1X53, 14.1X53-D130 eta 14.1X53-D49 baino lehenagoko bertsioak
    - 14.1X53 , 14.1X53-D48 baino lehenagoko bertsioak EX / QFX seriean
    - 15.1, bertsio hauek baino lehenagokoak: 15.1F6-S12, 15.1R7-S3 eta 15.1R7-S4
    - 15.1, 15.1R4-S9 eta 15.1R7-S2 baino lehenagoko bertsioak
    - 15.1F6, 15.1F6-S11 baino lehenagoko bertsioak
    - 15.1X49, ondoren doazen bertsioak baino lehenagokoak SRX seriean: 15.1X49-D141, 15.1X49-D144, 15.1X49-D150
    - 15.1X49, 15.1X49-D160 bertsioa baino lehenagokoak SRX340 eta SRX345 serieetan
    - 15.1X49, 15.1X49-D160 baino lehenagoko bertsioak SRX5000 seriean
    - 15.1X49, bertsio hauek baino lehenagokoak: 15.1X49-D160, 15.1X49-D161, 15.1X49-D170, 15.1X49-D171, 15.1X49-D180
    - 15.1X49, 15.1X49-D75 baino lehenagoko bertsioak SRX seriean.
    - 15.1X53, 15.1X53-D234 bertsioa baino lehenagokoak QFX5200 / QFX5110 serieetan
    - 15.1X53, 15.1X53-D235 bertsioa baino lehenagokoak QFX5000, EX4300, EX4600 serieetan
    - 15.1X53, bertsio hauek baino lehenagokoak: 15.1X53-D236, 15.1X53-D495, 15.1X53-D496, 15.1X53-D591, 15.1X53-D69, 15.1X53-D68
    - 15.1X53, 15.1X53-D471 eta 15.1X53-D490 baino lehenagoko bertsioak NFX seriean
    - 15.1X53, 15.1X53-D590 bertsioa baino lehenagokoak EX2300 / EX3400 serieetan
    - 15.1X53, 15.1X53-D68 baino lehenagoko bertsioak QFX10K seriean
    - 15.1X54, ACX seriean
    - 16.1, honakoak baino lehenagoko bertsioak: 16.1R3-S10, 16.1R4-S12, 16.1R4-S11, 16.1R6-S5, 16.1R6-S6, 16.1R7-S4, 16.1R7-S3, 16.1R7, 16.1R7-S5, 16.1R7-S1
    - 16.1X65, 16.1X65-D49 eta 16.1X65-D48 baino lehenagoko bertsioak
    - 16.2, bertsio hauek baino lehenagokoak: 16.2R2-S6, 16.2R2-S7, 16.2R2-S8, 16.2R2-S9, 16.2R3
    - 17.1, honako hauek baino lehenagoko bertsioak: 17.1R2-S10, 17.1R2-S8, 17.1R2-S7, 17.1R3

- 17.1, 17.1R3 bertsioa baino lehenagokoak QFX5000, EX4300, EX4600 serieetan
- 17.2, honako hauek baino lehenagoko bertsioak: 17.2R1-S7, 17.2R1-S8, 17.2R3, 17.2R3-S1
- 17.2, 17.2R3 bertsioa baino lehenagokoak QFX5000, EX4300, EX4600 serieetan
- 17.2X75, bertsio hauek baino lehenagokoak: 17.2X75-D92, 17.2X75-D102, 17.2X75-D110
- 17.3, SRX340 / SRX345 serieetan
- 17.3, bertsio hauek baino lehenagokoak: 17.3R2, 17.3R2-S2, 17.3R3
- 17.3, 17.3R3-S2 eta 17.3R4 baino lehenagoko bertsioak QFX5000, EX4300, EX4600 serieetan
- 17.3, bertsio hauek baino lehenagokoak: 17.3R3-S3, 17.3R3-S4, 17.3R4
- 17.4, honakoak baino lehenagoko bertsioak: 17.4R1-S1, 17.4R2-S2, 17.4R2-S3, 17.4R2-S4, 17.4R1-S4, 17.4R1-S6, 17.4R1-S7, 17.4R2, 17.4R2-S3, 17.4R3
- 17.4, 17.4R2-S1 eta 17.4R3 baino lehenagoko bertsioak QFX5000, EX4300, EX4600 serieetan
- 17.4, 17.4R2-S3 eta 17.4R3 baino lehenagoko bertsioak SRX340 / SRX345 serieetan
- 18.1, bertsio hauek baino lehenagokoak: 18.1R2, 18.1R3-S1, 18.1R3-S2, 18.1R3-S3, 18.1R3-S4, 18.1R4
- 18.1, 18.1R3-S1 bertsioa baino lehenagokoak SRX340 / SRX345 serieetan
- 18.1, 18.1R3-S1 eta 18.1R4 baino lehenagoko bertsioak QFX5000, EX4300, EX4600 serieetan
- 18.2, 18.2R1-S5 eta 18.2R2-S1 baino lehenagoko bertsioak
- 18.2, 18.2R2 bertsioa baino lehenagokoak QFX5000, EX4300, EX4600 serieetan
- 18.2, 18.2R2 bertsioa baino lehenagokoak SRX340 / SRX345 serieetan
- 18.2, honako hauek baino lehenagoko bertsioak: 18.2R2, 18.2R2-S2, 18.2R2-S3, 18.2R3
- 18.2, 18.2R1-S2 eta 18.2R2 baino lehenagoko bertsioak EX4300-MP seriean
- 18.2X75, bertsio hauek baino lehenagokoak: 18.2X75-D10, 18.2X75-D30, 18.2X75-D40
- 18.2X75, 18.2X75-D30 bertsioa baino lehenagokoak QFX5000, EX4300, EX4600 serieetan
- 18.3, bertsio hauek baino lehenagokoak: 18.3R1-S1, 18.3R1-S3, 18.3R1-S2, 18.3R1-S3, 18.3R2
- 18.3, 18.3R1-S2 eta 18.3R2 baino lehenagoko bertsioak SRX340 / SRX345 serieetan
- 18.3, 18.3R2 bertsioa baino lehenagokoak QFX5000, EX4300, EX4600 serieetan
- 18.4, bertsio hauek baino lehenagokoak: 18.4R1-S1, 18.4R1-S2, 18.4R2
- Aurreko bertsio guztiak 12.3 barne

Azalpena:

Juniperrek 17 segurtasun ohartarazpen argitaratu ditu. Horietan 17 ahultasunen berri ematen da, 1 larritasun kritikokoa, 9 kritikotasun altukoak eta gainerakoak ertainak edo baxuak.

Konponbidea:

- Kaltetutako produktu bakoitzari buruzko informazio xehea eskuratzeko "Erreferentziak" atala bisitatzea.

Xehetasuna:

- Larritasun kritikoko ahultasunak Junos Networks Junos OS-i eragiten dio QFX5000, EX4300, EX4600 serieetan. Baliagarriak diren BGP edo IPv6 BFD paketeen segida zehatz batek pilan oinarritutako bufferraren gainezkatzea eragin dezake Junos OS Forwarding Engine Manager-en (FXPC), QFX5000, EX4300 eta EX4600 serieetako gailuetan. Arazo honek daemon fxpc-ren ustekabeko itxiera eragin lezake edo kodearen urruneko exekuzioa. Ahultasun horretarako CVE-2019-0008 identifikatzailea erabili da.

Gainerako ahultasunek ondokoa eragin lezakete:

- Firewall-a saihestea, CVE-2019-0036 eta CVE-2019-0042 identifikatzaileak esleitu zaizkio.
- Zerbitzuaren ukapena (DoS), ondoko identifikatzaileak esleitu zaizkio: CVE-2019-0044, CVE-2019-0031, CVE-2019-0033, CVE-2019-0037, CVE-2019-0019, CVE-2019-0028, CVE-2019-0043, CVE-2019-0038, CVE-2019-0040 eta CVE-2019-0042.
- Testu lauan gordetako kredentzialak, CVE-2019-0032 identifikatzailea esleitu zaio.
- Informazio pribilegiaturako sarbidea, CVE-2019-0034 identifikatzailea esleitu zaio.
- Autentifikazioa saihestea, CVE-2019-0035 identifikatzailea esleitu zaio.
- Kredentzialak eskuratzea indarraren indarrez, CVE-2019-0039 identifikatzailea esleitu zaio.
- Aginte mahairako sarbidea lortzea loopback interfazearen bidez, CVE-2019-0041 identifikatzailea esleitu zaio.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun IBMren API Connect-en

Argitalpen data: 2019/04/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IBM API Connect, 5.0.0.0tik 5.0.8.6ra bitarteko bertsioak

Azalpena:

API Connect-ek dituen bi ahultasunen berri eman da, bat komandoen injekzio erakoa eta bestea fitxategi lokalen inklusio erakoa (LFI, *Local File Inclusion*).

Konponbidea:

- IBMk bi ahultasunak konpondu ditu 5.0.8.6 iFix bertsioan.

Xehetasuna:

- IBM API Connect Developer Portal ahula da komandoen injekzioaren aurrean. Bereziki diseinatutako eskaera bat egiten duen erasotzaile batek kode arbitrarioa exekuta lezake zerbitzarian eta sistemara sarbide osoa lortu. Ahultasun horretarako CVE-2019-4202 identifikatzailea erreserbatu da.
- Aplikazioen garatzaileek IBM API Connect Developer Portal balia dezakete host-aren sistema eragiletik fitxategi arbitrarioak deskargatzeko eta SSRF (*Server Side Request Forgery*) erasoak egiteko. Ahultasun horretarako CVE-2019-4203 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Mugaz kanpoko irakurketa erako hainbat ahultasun VMware-ren produktuetan

Argitalpen data: 2019/04/12

Garrantzia: Handia

Kaltetutako baliabideak:

- VMware vSphere ESXi (ESXi), honako bertsioak:
  - 6.5
  - 6.7
- VMware Workstation Pro / Player (Workstation), honako bertsioak:
  - 15.X
  - 14.X
- VMware Fusion Pro / Fusion (Fusion), honako bertsioak:
  - 11.x
  - 10.x

Azalpena:

VMwarek bere produktu batzuei eragiten dieten mugez kanpoko irakurketa erako 3 ahultasun aurkitu ditu, kritikotasun altukoak.

Konponbidea:

VMwarek ahultasun horiek arintzen dituzten hainbat eguneraketa argitaratu ditu, kaltetutako produktuaren eta bertsioaren arabera.

- ESXiren honako bertsioak:
  - 6.7 bertsioaren kasuan, ESXi670-201904101-SG partxea aplikatzea
  - 6.5 bertsioaren kasuan, ESXi650-201903001 partxea aplikatzea
- Workstation Pro-ren kasuan,14.1.6 edo 15.0.3 bertsioetara eguneratzea
- Workstation Player-en kasuan,14.1.6 edo 15.0.3 bertsioetara eguneratzea
- Fusion Pro / Fusion-en kasuan, 10.1.6 o 11.0.3 bertsioetara eguneratzea

Xehetasuna:

- Vertex shader funtzionaltasunak duen mugez kanpoko irakurketa erako ahultasun bat baliatuz, erasotzaile batek, 3D grafikoak gaituta dituen makina birtual batera sartuko balitz, informazioa heda lezake edo zerbitzuaren ukapen egoera eragin lezake makina birtualean. Ahultasun horretarako CVE-2019-5516 identifikatzailea erreserbatu da.
- Shader translator-ek dituen mugez kanpoko irakurketa erako hainbat ahultasun baliatuz, erasotzaile batek, 3D grafikoak gaituta dituen makina birtual batera sartuko balitz, informazioa heda lezake edo zerbitzuaren ukapen egoera eragin lezake makina birtualean. Ahultasun horretarako CVE-2019-5517 identifikatzailea erreserbatu da.
- Mugez kanpoko irakurketa erako ahultasun bat baliatuz, erasotzaile batek, 3D grafikoak gaituta dituen makina birtual batera sartuko balitz, informazioa heda lezake edo zerbitzuaren ukapen egoera eragin lezake makina birtualean. Ahultasun horretarako CVE-2019-5520 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Eguneraketa kritikoak Oraclen (2019ko apirila)

Argitalpen data: 2019/04/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Agile Recipe Management for Pharmaceuticals, 9.3.3 eta 9.3.4 bertsioak
- Enterprise Manager Base Platform, 12.1.0.5.0, 13.2.0.0.0 eta 13.3.0.0.0 bertsioak
- Enterprise Manager Ops Center, 12.3.3 bertsioa
- FMW Platform, 12.2.1.3.0 bertsioa
- Instantis EnterpriseTrack, 17.1, 17.2 eta 17.3 bertsioak
- JD Edwards EnterpriseOne Tools, 9.2 bertsioa
- JD Edwards World Technical Foundation, A9.2, A9.3.1 eta A9.4 bertsioak
- MICROS Lucas, 2.9.5.6 eta 2.9.5.7 bertsioak
- MICROS Relate CRM Software, 11.4 bertsioa
- MICROS Retail-J, 12.1.2 bertsioa
- MySQL Connectors, 5.3.12 eta lehenagoko bertsioak, eta 8.0.15 eta lehenagokoak
- MySQL Enterprise Backup, 3.12.3 eta lehenagoko bertsioak, eta 4.1.2 eta lehenagokoak
- MySQL Enterprise Monitor, 4.0.8 eta lehenagoko bertsioak, 8.0.14 eta lehenagokoak
- MySQL Server, 5.6.43 eta lehenagoko bertsioak, 5.7.25 eta lehenagokoak, 8.0.15 eta lehenagokoak
- Oracle Agile PLM, 9.3.3, 9.3.4 eta 9.3.5 bertsioak
- Oracle API Gateway, 11.1.2.4.0 bertsioa
- Oracle Application Testing Suite, 13.3.0.1 bertsioa
- Oracle AutoVue 3D Professional Advanced, 21.0.0 eta 21.0.1 bertsioak
- Oracle Banking Platform, 2.4.0, 2.4.1, 2.5.0 eta 2.6.0 bertsioak
- Oracle Berkeley DB, 6.138 baino lehenagoko bertsioak eta 18.1.32 baino lehenagokoak
- Oracle BI Publisher, 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak
- Oracle Business Intelligence Enterprise Edition, 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak
- Oracle Business Process Management Suite, 11.1.1.9.0, 12.1.3.0.0 eta 12.2.1.3.0 bertsioak
- Oracle Business Transaction Management, 12.1.0 bertsioa
- Oracle Commerce Merchandising, 11.2.0.3 bertsioa
- Oracle Commerce Platform, 11.2.0.3 eta 11.3.1 bertsioak
- Oracle Communications Application Session Controller, 3.7.1 eta 3.8.0 bertsioak
- Oracle Communications EAGLE Application Processor, 16.1.0 eta 16.2.0 bertsioak
- Oracle Communications EAGLE LNP Application Processor, 10.0, 10.1 eta 10.2 bertsioak
- Oracle Communications Instant Messaging Server, 10.0.1 bertsioa
- Oracle Communications Interactive Session Recorder, 6.0, 6.1 eta 6.2 bertsioak
- Oracle Communications LSMS, 13.1, 13.2 eta 13.3 bertsioak

- Oracle Communications Messaging Server, 8.0 eta 8.1 bertsioak
- Oracle Communications Operations Monitor, 3.4 eta 4.0 bertsioak
- Oracle Communications Policy Management, 12.1, 12.2, 12.3 eta 12.4 bertsioak
- Oracle Communications Pricing Design Center, 11.1 eta 12.0 bertsioak
- Oracle Communications Service Broker, 6.0 bertsioa
- Oracle Communications Service Broker Engineered System Edition, 6.0 bertsioa
- Oracle Communications Session Border Controller, 8.0.0, 8.1.0 eta 8.2.0 bertsioak
- Oracle Communications Unified Inventory Management, 7.3.2, 7.3.4, 7.3.5 eta 7.4.0 bertsioak
- Oracle Configuration Manager, 12.1.0 bertsioa
- Oracle Configurator, 12.1 eta 12.2 bertsioak
- Oracle Data Integrator, 11.1.1.9.0 eta 12.2.1.3.0 bertsioak
- Oracle Database Server, 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c eta 19c bertsioak
- Oracle E-Business Suite, 0.9.8, 1.0.0, 1.0.1, 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 eta 12.2.8 bertsioak
- Oracle Endeca Information Discovery Integrator, 3.2.0 bertsioa
- Oracle Enterprise Communications Broker, 3.0.0 eta 3.1.0 bertsioak
- Oracle Enterprise Operations Monitor, 3.4 eta 4.0 bertsioak
- Oracle Enterprise Session Border Controller, 8.0.0, 8.1.0 eta 8.2.0 bertsioak
- Oracle Financial Services Analytical Applications Infrastructure, 7.3.3 - 7.3.5 eta 8.0.0 - 8.0.7 bertsioak
- Oracle Financial Services Asset Liability Management, 8.0.4 - 8.0.7 bertsioak
- Oracle Financial Services Data Integration Hub, 8.0.5 - 8.0.7 bertsioak
- Oracle Financial Services Funds Transfer Pricing, 8.0.4 - 8.0.7 bertsioak
- Oracle Financial Services Hedge Management y IFRS Valuations, 8.0.4 - 8.0.7 bertsioak
- Oracle Financial Services Liquidity Risk Management, 8.0.2 - 8.0.6 bertsioak
- Oracle Financial Services Loan Loss Forecasting and Provisioning, 8.0.2 - 8.0.7 bertsioak
- Oracle Financial Services Market Risk Measurement and Management, 8.0.5, 8.0.6 bertsioak
- Oracle Financial Services Profitability Management, 8.0.4 - 8.0.6 bertsioak
- Oracle Financial Services Reconciliation Framework, 8.0.5, 8.0.6 bertsioak
- Oracle FLEXCUBE Private Banking, 2.0.0.0, 2.2.0.1, 12.0.1.0, 12.0.3.0 eta 12.1.0.0 bertsioak
- Oracle Fusion Middleware MapViewer, 12.2.1.3.0 bertsioa
- Oracle Health Sciences Data Management Workbench, 2.4.8 bertsioa
- Oracle Healthcare Master Person Index, 3.0 eta 4.0 bertsioak
- Oracle Hospitality Cruise Dining Room Management, 8.0.80 bertsioa
- Oracle Hospitality Cruise Fleet Management, 9.0.11 bertsioak
- Oracle Hospitality Guest Access, 4.2.0 eta 4.2.1 bertsioak
- Oracle Hospitality Reporting and Analytics, 9.1.0 bertsioa
- Oracle HTTP Server, 12.2.1.3.0 bertsioa
- Oracle Identity Analytics, 11.1.1.5.8 bertsioak
- Oracle Java SE, 7u211, 8u202, 11.0.2 eta 12 bertsioak
- Oracle Java SE Embedded, 8u201 bertsioa
- Oracle JDeveloper, 11.1.1.9.0, 12.1.3.0.0 eta 12.2.1.3.0 bertsioak
- Oracle Knowledge, 8.5.1.0 - 8.5.1.7, 8.6.0 eta 8.6.1 bertsioak
- Oracle Managed File Transfer, 12.1.3.0.0 eta 12.2.1.3.0 bertsioak
- Oracle Outside In Technology, 8.5.3 eta 8.5.4 bertsioak
- Oracle Real-Time Scheduler, 2.3.0 bertsioa
- Oracle Retail Allocation, 15.0.2 bertsioa
- Oracle Retail Convenience Store Back Office, 3.6 bertsioa
- Oracle Retail Customer Engagement, 16.0 eta 17.0 bertsioak
- Oracle Retail Customer Management and Segmentation Foundation, 16.0, 17.0 eta 18.0 bertsioak
- Oracle Retail Invoice Matching, 12.0, 13.0, 13.1, 13.2, 14.0, 14.1 eta 15.0 bertsioak
- Oracle Retail Merchandising System, 15.0 eta 16.0 bertsioak
- Oracle Retail Order Broker, 5.1, 5.2, 15.0 eta 16.0 bertsioak
- Oracle Retail Point-of-Service, 13.4, 14.0 eta 14.1 bertsioak
- Oracle Retail Workforce Management Software, 1.60.9.0.0 bertsioa
- Oracle Retail Xstore Point of Service, 7.0 eta 7.1 bertsioak
- Oracle Secure Global Desktop, 5.4 bertsioa
- Oracle Service Bus, 11.1.1.9.0, 12.1.3.0.0 eta 12.2.1.3.0 bertsioak
- Oracle SOA Suite, 11.1.1.9.0, 12.1.3.0.0 eta 12.2.1.3.0 bertsioak
- Oracle Solaris, 10 eta 11 bertsioak
- Oracle Traffic Director, 11.1.1.9.0 bertsioa
- Oracle Transportation Management, 6.3.7, 6.4.2 eta 6.4.3 bertsioak
- Oracle Tuxedo, 12.1.1.0.0 bertsioa
- Oracle Utilities Framework, 2.2.0, 4.2.0.2.0, 4.2.0.3.0, 4.3.0.2.0, 4.3.0.3.0, 4.3.0.4.0, 4.3.0.5.0, 4.3.0.6.0 eta 4.4.0.0.0 bertsioak
- Oracle Utilities Mobile Workforce Management, 2.3.0 bertsioa
- Oracle Utilities Network Management System, 1.12.0.3 bertsioa
- Oracle VM VirtualBox, 5.2.28 baino lehenagoko bertsioak eta 6.0.6 baino lehenagokoak
- Oracle WebCenter Portal, 12.2.1.3.0 bertsioa
- Oracle WebCenter Sites, 12.2.1.3.0 bertsioa
- Oracle WebLogic Server, 10.3.6.0.0, 12.1.3.0.0 eta 12.2.1.3.0 bertsioak
- OSS Support Tools, 19.1 bertsioa
- PeopleSoft Enterprise ELM, 9.2 bertsioa
- PeopleSoft Enterprise ELM Enterprise Learning Management, 9.2 bertsioa
- PeopleSoft Enterprise HCM Talent Acquisition Manager, 9.2 bertsioa
- PeopleSoft Enterprise HRMS, 9.2 bertsioa
- PeopleSoft Enterprise PeopleTools, 8.55, 8.56 eta 8.57 bertsioak
- PeopleSoft Enterprise PT PeopleTools, 8.55, 8.56 eta 8.57 bertsioak
- Primavera P6 Enterprise Project Portfolio Management, 8.4, 15.1, 15.2, 16.1, 16.2, 17.7 - 17.12 eta 18.8 bertsioak
- Primavera Unifier, 16.1, 16.2, 17.7 - 17.12 eta 18.8 bertsioak
- Siebel Applications, 19.3 bertsioa

Azalpena:

Oraclek partxedun eguneraketa kritiko bat argitaratu du, hainbat produkturi eragiten dieten ahultasunak zuzentzeko.

Konponbidea:

Kaltetutako produktuen arabera, dagozkien partxeak aplikatzea. Eguneraketak deskargatzeko informazioa Oraclek argitaratutako segurtasun buletinean lor daiteke.

Xehetasuna:

Eguneraketa horrek 297 ahultasun konpontzen ditu guztira, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna Erreferentzien atalean dagoen Oracleren loturan kontsulta daiteke.

Etiketak:

Hainbat ahultasun BIND-en

Argitalpen data: 2019/04/25

Garrantzia: Handia

Kaltetutako baliabideak:

- BIND, 9.9.0tik 9.10.8-P1era bitarteko bertsioak, 9.11.0tik 9.11.6ra bitartekoak, 9.12.0tik 9.12.4ra bitartekoak eta 9.14.0.
- BIND 9 Supported Preview Edition, 9.9.3-S1tik 9.11.5-S3ra bitarteko bertsioak eta 9.11.5-S5.9.13 garapen adarreko 9.13.0tik 9.13.7ra bitarteko bertsioak ere kaltetuta daude. BIND 9.9.0 baino lehenagoko bertsioak ez ditu ebaluatu CVE-2018-5743 ahultasunak.
- BIND Supported Preview Edition, 9.10.5-S1etik 9.11.5-S5era bitarteko bertsioak.

Azalpena:

BINDek dituen hainbat ahultasunen berri argitaratu da, 1 larritasun altukoa eta 2 larritasun ertainekoak.

Konponbidea:

Kaltetutako bertsioaren arabera dagokion bertsiora eguneratzea.

- BIND 9.11.5-S6
- BIND 9.11.6-S1
- BIND 9.11.6-P1
- BIND 9.12.4-P1
- BIND 9.14.1

Xehetasuna:

- Diseinutik BINDek mugatu egiten du aldi berean konekta daitekeen TCP bezeroen kopurua. Parametro hori alda daiteke baina aldatzen ez den bitartean balio kontserbadorea dauka. Kodeak duen akats bat baliatuz, erasotzaile batek aldi bereko TCP konexioen kopurua mugaz gain handitu lezake. Horrela sareko konexioetarako eskuragarri dauden fitxategien deskribatzaileen multzoa agortzea eragin lezake. Ahultasun horretarako CVE-2018-5743 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako ondoko identifikatzaileak erreserbatu dira: CVE-2019-6467 eta CVE-2019-6468.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun TIBCOren produktuetan

Argitalpen data: 2019/04/25

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- TIBCO ActiveMatrix BPM, 4.2.0 eta lehenagoko bertsioak.
- TIBCO Silver Fabric-erako TIBCO ActiveMatrix BPM Distribution, 4.2.0 eta lehenagoko bertsioak.
- TIBCO ActiveMatrix Policy Director, 1.1.0 eta lehenagoko bertsioak.
- TIBCO ActiveMatrix Service Bus, 3.3.0 eta lehenagoko bertsioak.
- TIBCO ActiveMatrix Service Grid, 3.3.1 eta lehenagoko bertsioak.
- TIBCO Silver Fabric-erako TIBCO ActiveMatrix Service Grid Distribution, 3.3.0 eta lehenagoko bertsioak.
- ActiveMatrix BPM-rako TIBCO Silver Fabric Enabler, 1.4.1 eta lehenagoko bertsioak.
- ActiveMatrix Service Grid-erako TIBCO Silver Fabric Enabler, 1.3.1 eta lehenagoko bertsioak.
- Administratzailearen web interfazeko osagaiak, administrazio zerbitzaria, web zerbitzari administratzailea, bezeroaren lan area, bezeroaren gune irekia, aplikazioen garapen bezeroa eta REST API.

Azalpena:

TIBCOk bere hainbat produkturi eragiten dieten 6 ahultasunen berri eman du. Horien bitartez erasotzaile batek hainbat eraso mota egin litzake: XSS, CSRF, kodearen urruneko exekuzioa, informazio konfidentziala deskargatzea autentifikaziorik gabe, pribilegioak eskalatzea edo birbideratze irekia.

Konponbidea:

- TIBCO ActiveMatrix BPMren kasuan, 4.3.0 edo goragoko bertsiora eguneratzea.
- TIBCO Silver Fabric-erako TIBCO ActiveMatrix BPM Distribution-en kasuan, 4.3.0 edo goragoko bertsiora eguneratzea.
- TIBCO ActiveMatrix Policy Director-en kasuan, 2.0.0 edo goragoko bertsiora eguneratzea. Produktu hau 2021. urtearen hasieran erretiratzea aurreikusita dagoenez, arren eskatzen zaie bezeroei TIBCOren laguntza teknikoaren zerbitzuarekin harremanetan jartzea arazoa konpontzeko beste modu batzuk aztertzearren.
- TIBCO ActiveMatrix Service Bus-en kasuan, 3.4.0 edo goragoko bertsiora eguneratzea.
- TIBCO ActiveMatrix Service Grid-en kasuan, 3.4.0 edo goragoko bertsiora eguneratzea.
- TIBCO Silver Fabric-erako TIBCO ActiveMatrix Service Grid Distribution-en kasuan, 3.4.0 edo goragoko bertsiora eguneratzea.
- ActiveMatrix BPMrako TIBCO Silver Fabric Enabler-en kasuan, 1.4.2 edo goragoko bertsiora eguneratzea.
- ActiveMatrix Service Grid-erako TIBCO Silver Fabric Enabler-en kasuan, 1.3.2 edo goragoko bertsiora eguneratzea.

Xehetasuna:

- Pribilegiorik gabeko urruneko erasotzaile batek sarbide osoa lor lezake TIBCO ActiveMatrix Administrator-en web interfazeko gaitasun guztietara XSS edo CSRF bidez. Ahultasun horretarako CVE-2019-8991 identifikatzailea erabili da.
- Pribilegiorik gabeko erabiltzaile batek kodea karga lezake, eta horrela kode arbitrarioa exekuta lezake ActiveMatrix Service Grid-en nodoetan. Ahultasun horretarako CVE-2019-8992 identifikatzailea erabili da.
- Autentifikaziorik gabeko erabiltzaile batek kredentzialen informazioa duen fitxategi bat deskarga lezake. Ahultasun horretarako CVE-2019-8993 identifikatzailea erabili da.
- Autentifikatutako erabiltzaile batek sistemako beste erabiltzaile batzuk engaina litzake asmo gaiztoko webguneak bisita ditzaten. Ahultasun horretarako CVE-2019-8994 identifikatzailea erabili da.

- Erasotzaile batek asmo gaiztoko URL bat erabil lezake erabiltzaile bat engainatzeko eta webgune jakin bat bisita dezan lortzeko. Ahultasun horretarako CVE-2019-8995 identifikatzailea erabili da.
- Pribilegiorik gabeko urruneko erasotzaile batek kaltetutako ActiveMatrix BPM osagaiek agerian utzitako APIetara sarbide osoa lor lezake. Ahultasun horretarako CVE-2019-11203 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Host-en goiburuen injekzio erako ahultasuna IBM StoredIQ-n

Argitalpen data: 2019/04/29

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM StoredIQ, 7.6.0.0tik 7.6.0.18ra bitarteko bertsioak

Azalpena:

IBM StoredIQ-ri StoredIQ Dataserver-en host-en goiburuen injekzio erako ahultasun batek eragin liezaioke.

Konponbidea:

- Ez da beharrezkoa inolako zuzenketarik egitea baina beharrezkoa da konfigurazioa eguneratzea, aipatutako IBMren ohartarazpeneko Workarounds and Mitigations atalean aipatzen den moduan.

Xehetasuna:

- IBM StoredIQ-k urruneko erasotzaile bati phishing erasoak egitea ahalbidetu liezaioke, birbideratze irekiko eraso bat erabiliz. Biktima bat konbentzitu ondoren bereziki diseinatutako webgune bat bisita dezan, urruneko erasotzaile batek ahultasun hau balia lezake erakutsitako URLa faltsutuz eta erabiltzaile bat fidagarria zirudien asmo gaiztoko webgune batera birbideratuz. Horri esker erasotzaileak informazio sentikorra eskura lezake edo biktimaren aurkako eraso berriak egin. Ahultasun horretarako CVE-2019-4166 identifikatzailea erreserbatu da.

Etiketak: IBM, Ahultasuna

Kodearen urruneko exekuzio erako ahultasuna Oracle WebLogic Server-en

Argitalpen data: 2019/04/29

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Oracle WebLogic Server, 10.3.6.0.0 eta 12.1.3.0.0 bertsioak

Azalpena:

Oracle-k larritasun kritikoko ahultasun baten berri eman du, bere Oracle WebLogic Server produktuan kodearen urruneko exekuzioa ahalbidetzen duena. Dagoeneko badago ahultasun hori nola balia daitekeen erakusten duen kontzeptu froga bat.

Konponbidea:

- Oracle-k erabiltzaileei lotura bat eskaini die eskuragarri dauden partxeei eta horiek instalatzeko argibideei buruzko informazioa jasotzen duen dokumentazioa lortzeko.
- Arintze neurri modura, ahulak diren «wls9_async_response.war» eta «wls-wsat.war» moduluak desgaitzea, edo «/ _async / *» eta «/ wls-wsat / *» URLetarako sarbidea galaraztea gomendatzen dute Oracle WebLogic-en instalazioen barnean.

Xehetasuna:

- Oracle WebLogic Server-ek duen deserializazio erako ahultasun bat baliatuz, erasotzaile batek urrunetik eta autentifikaziorik gabe kodea exekuta lezake. Ahultasun horretarako CVE-2019-2725 identifikatzailea erabili da.

Etiketak: Eguneraketa, Oracle, Ahultasuna

Autentifikazio jauzia Citrix-en XenMobile Server-en

Argitalpen data: 2019/04/29

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Citrix XenMobile Server, ondoko bertsioak:
  - *Rolling Patch 3* baino lehenagoko 10.9.0 bertsioak.
  - *Rolling Patch 6* baino lehenagoko 10.8.0 bertsioak.

Azalpena:

Autentifikazioaren jauzi erako larritasun kritikoko ahultasun bat aurkitu da Citrix XenMobile Server-en.

Konponbidea:

- Citrix-ek ahultasun hori arintzen duten eguneraketak argitaratu ditu bere erabiltzaile erregistratuentzat:
-
    - Citrix XenMobile Server 10.9.0 *Rolling Patch 3*
    - Citrix XenMobile Server 10.8.0 *Rolling Patch 6*

Xehetasuna:

- Ahultasuna baliatuz erasotzaile batek autentifikazio jauzia egin lezake Citrix XenMobile Server-en, eta *Mobile Device Management*-en (MDM) erregistratutako edozein gailutan ekintzak egin litzake. Ahultasun horretarako CVE-2018-18571 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

DoS erako ahultasuna Liferay-n

Argitalpen data: 2019/04/29

Garrantzia: Handia

Kaltetutako baliabideak:

- com.liferay.faces.bridge.impl-4.1.2
- com.liferay.faces.bridge.impl-3.1.0
- liferay-faces-bridge-impl-4.2.5-ga6
- liferay-faces-bridge-impl-3.2.5-ga6
- liferay-faces-bridge-impl-3.1.5-ga6
- liferay-faces-bridge-impl-3.0.5-ga6
- liferay-faces-bridge-impl-3.0.5-legacy-ga6
- com.liferay.faces.bridge.impl-4.1.2
- com.liferay.faces.bridge.impl-3.1.0
- liferay-faces-bridge-impl-4.2.5-ga6
- liferay-faces-bridge-impl-3.2.5-ga6
- liferay-faces-bridge-impl-3.1.5-ga6
- liferay-faces-bridge-impl-3.0.5-ga6
- liferay-faces-bridge-impl-3.0.5-legacy-ga6
- com.liferay.faces.bridge.impl-4.1.2
- com.liferay.faces.bridge.impl-3.1.0
- liferay-faces-bridge-impl-4.2.5-ga6
- liferay-faces-bridge-impl-3.2.5-ga6

Bertsio hauetakoren batekin bateragarriak:

- Liferay Portal 5.2
- Liferay Portal 6.0
- Liferay Portal 6.1
- Liferay Portal 6.2
- Liferay Portal 7.0
- Liferay Portal 7.1
- Pluto Portal 2.0

Xehetasun gehiagotarako erreferentziak ikusi.

Azalpena:

Liferay Portal CE-k dituen hainbat ahultasunek zerbitzuaren ukapen egoera eragin dezakete fitxategi handiak kargatzearen bitartez.

Konponbidea:

- Kaltetutako bertsioaren arabera partxe egokia aplikatzea.

Xehetasuna:

- Liferay Faces Bridge-rekin batera erabiltzen denean, fitxategien kargaren egiaztapena saihestu egin daiteke. Horrek ahalbidetzen du fitxategi oso handiak kargatu ahal izatea zerbitzuaren ukapen erako (Dos) eraso batean. Egiaztatzen ez diren fitxategiak ondokoak dira:
-
    - PrimeFaces 6.2 p:fileUpload.
    - RichFaces rich:fileUpload.
    - com.liferay.faces.bridge.uploadedFileMaxSize on IceFaces ace:fileEntry.
    - com.liferay.faces.util.uploadedFileMaxSize con alloy:inputFile en Portlets.
    - IceFaces 1.8 ice:inputFile.

Etiketak: Ahultasuna