2018ko Uztailaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun IBMren Db2-n

Argitalpen data: 2018/07/09

Garrantzia: Handia

Kaltetutako baliabideak:

IBM Db2ren bertsio hauek:

- V9.7.
- V10.1.
- V10.5.
- V11.1.

Azalpena:

IBMk kritikotasun altuko 3 ahultasun aurkitu ditu Db2-n. Horien bitartez, erasotzaile lokal batek pribilegioen igoera lor lezake eta kode arbitrarioa exekutatu.

Konponbidea:

IBMk erabiltzaileen eskura jarri ditu ahultasunak konpontzen dituzten segurtasun eguneraketak, kaltetutako Db2ren bertsio eta plataforma bakoitzaren arabera.

Db2ren eguneraketak honakoak dira:

- V9.7 FP11, V9.7 bertsioetarako.
- V10.1 FP6, V10.1 bertsioetarako.
- V10.5 FP9, V10.5 bertsioetarako.
- V11.1.3 iFix001, V11.1.3 bertsioetarako.

Deskargetarako loturak Erreferentziak atalean daude eskuragarri.

Xehetasuna:

- Db2n fidagarriak izan ez daitezkeen bideetan zehar liburutegien karga baliatuz, sisteman pribilegio baxuak dituen erasotzaile batek sarbide osoa lor lezake Db2ren instantzia kontura. Ahultasun horretarako CVE-2018-1487 identifikatzailea erreserbatu da.
- Windowsen Db2 Administration Server-ek dituen hainbat ahultasun baliatuz, erabiltzaile lokal batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2018-1458 identifikatzailea erreserbatu da.
- db2support tresnak katea formatuko ahultasun bat dauka. Hori baliatuz erabiltzaile lokal batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2018-1566 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

2018ko uztaileko Microsoften segurtasun buletina

Argitalpen data: 2018/07/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office, Microsoft Office Services eta Web Apps
- ChakraCore

- Adobe Flash Player
- . NET Framework
- ASP.NET
- Microsoft Research JavaScript Cryptography Library
- Skype for Business and Microsoft Lync
- Visual Studio
- Microsoft Wireless Display Adapter V2 Software
- PowerShell Editor Services
- Visual Studio Code-rako PowerShell Extension
- Active Directory Federation Services-erako Web Customizations

Azalpena:

Microsoftek hilean behin segurtasun eguneraketei buruz argitaratzen duen argitalpeneko hile honetako alean 50 ahultasun jaso dira. Horietatik 17 kritiko gisa sailkatu dira eta 33 garrantzitsu gisa. Gainerako ahultasunak larritasun ertain edo baxukoak dira.

Konponbidea:

Dagokion eguneraketa instalatzea. Segurtasun eguneraketen instalazioaren informazio webgunean eguneraketa metodo ezberdinei buruz informatzen da.

Xehetasuna:

Uztailari dagokion segurtasun eguneraketen buletinean hainbat segurtasun ahultasun argitaratu dira, mota hauetakoak:

- Zerbitzuaren ukapena.
- Pribilegioen igoera.
- Informazioa ezagutaraztea.
- Kodearen urrutiko exekuzioa.
- Segurtasunari ihes egitea.
- Ordezpena.

Etiketak: Eguneraketa, Microsoft, Ahultasuna

Hainbat ahultasun Intel produktuetan

Argitalpen data: 2018/07/11

Garrantzia: Handia

Kaltetutako baliabideak:

- Intel Coreren 4., 5., 6. eta 7. belaunaldiko prozesadoreak
- Tiancoren oinarritutako firmwarea duten produktuak
- BMC firmwarea zerbitzari plaketan, zenbaketa moduluetan eta Intel sistemetan
- Intelen Python banaketa
- Intel CSME (Converged Security Management Engine)
- Intel Active Management Technology

Azalpena:

Intelek bere produktu batzuei eragiten dieten zazpi ahultasun argitaratu ditu, denak larritasun altukoak.

Konponbidea:

Intelen laguntza eta deskargen webgunea bisitatu zure produktuari dagokion partxea edo eguneraketa eskuratzeko.

Xehetasuna:

Ohartarazpen honetan azaldutako ahultasunak baliatuz, erasotzaile batek ondoko ekintzak egin litzake:

- Informazioa ezagutaraztea
- Pribilegioen eskalatzea
- Zerbitzuaren ukapena

Ahultasun horietarako ondoko identifikatzaileak erreserbatu dira: CVE-2017-5704, CVE-2018-3651, CVE-2018-3650, CVE-2018-3627, CVE-2018-3628, CVE-2018-3629 eta CVE-2018-3632.

Etiketak: Eguneraketa, Pribatutasuna, Ahultasuna

SAPen segurtasun eguneraketa 2018ko uztailean

Argitalpen data: 2018/07/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa
- SAP Internet Sales, 7.30,7.31, 7.32, 7.33 eta 7.54 bertsioak
- SAP Business Objects, 4.0tik 4.10era bitarteko bertsioak, 4.20tik 4.30era bitartekoak
- SAP Crystal Reports, Visual Studio .NETerako bertsioa, 2010eko bertsioa
- AP R/3 Enterprise Retail, EHP6 bertsioa
- SAP CrystalReports, Visual Studio .NETerako bertsioa, 2010eko bertsioa
- SAP BusinessObjects Business Intelligence Suite, 4.10 eta 4.20 bertsioak
- SAP Business Objects Enterprise, 4.0 eta 4.1 bertsioak
- SAP Gateway, honako bertsioak: SAP KERNEL 32 NUC, SAP KERNEL 32 Unicode, SAP KERNEL 64 NUC, SAP KERNEL 64 Unicode 7.21, 7.21EXT, 7.22 eta 7.22EXT; SAP KERNEL 7.21, 7.22, 7.45, 7.49 eta 7.53

- SAP MaxDB ODBC driver, 7.9.09.07 bertsioa
- SAP Internet Graphics Server (IGS); 7.20, 7.20EXT, 7.45, 7.49 eta 7.53 bertsioak
- NextLabs-eko (Java Policy Controller) SAP Dynamic Authorization Management (DAM), 7.7 eta 8.5 bertsioak
- SAP BusinessObjects Business Intelligence (BI Launchpad eta Central Management Console), 4.1, 4.2 eta 4.3 bertsioak
- Infrastructure for UI add-on for SAP NetWeaver (UI_Infra), SAP UI Implementation for Decoupled Innovations (UI_700): NW 7.00 Implementation, SAP User Interface Technology (SAP_UI), UI_Infra 1.0 bertsioak; SAP_UI 7.4, 7.5, 7.51 eta 7.52; UI_700 2.0

Azalpena:

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

Konponbidea:

SAPen laguntzarako webgunea bisitatu eta fabrikatzaileak adierazten dituen beharrezko eguneraketa edo partxeak instalatzea.

Xehetasuna:

SAPek segurtasun partxeei buruz argitaratzen duen hileroko komunikatuan 16 segurtasun ohar eman ditu ezagutzera. Horietatik 5 ohar lehenagotik argitaratutako segurtasun oharrei dagozkien eguneraketak dira, beste 1 larritasun kritikokoa da, beste 2 larritasun altukoak eta beste 13 larritasun ertainekoak.

Argitaratutako ahultasun motak ondokoak dira:

- Kode injekzioko 3 ahultasun
- Informazio zabalkundeko ahultasun bat
- Zerbitzuaren ukapeneko 3 ahultasun
- Cross-Site Scripting erako 2 ahultasun
- Baimenaren egiaztapen gabeziako ahultasun bat
- Beste tipologia batzuetako 3 ahultasun

Ahultasun garrantzitsuenak ondokoak dira:

- SAP R/3 Enterprise Retail-en baimenaren egiaztatze gabeziako ahultasun bat baliatuz, zerbitzu batera sarbidea lor liteke inolako baimen prozedurarik gabe, eta sarbide murriztua duen zerbitzuaren funtzionaltasuna erabil liteke. Horrek informazio zabalkundea, pribilegioen igoera eta beste eraso batzuk eragin litzake. Ahultasun horretarako CVE-2018-2436 kodea erreserbatu da.
- SAP CrystalReports-ek duen kodearen injekzio erako ahultasun bat baliatuz, komandoen exekuzioa lor liteke komandoa exekutatu zuen zerbitzuaren pribilegio berdinekin. Posible da SAP zerbitzariko fitxategien sistema batean kokatuta dauden fitxategi eta direktorio arbitrarioetara sarbidea lortzea, aplikazioaren iturburu kodea, konfigurazioa eta sistemaren fitxategi kritikoak barne. Kaltetutako SAP sistema batean gordetako informazio tekniko eta negozioari buruzko informazio kritikoa eskura daiteke. Ahultasun horretarako CVE-2018-2427 identifikatzailea erreserbatu da.
- SAP CrystalReports-ek duen Cross-Site Scripting erako ahultasun bat baliatuz, erasotzaile batek script gaiztoa injekta lezake orrialde batean, hura iraunkorki gordez orriaren gorputzean, eta horrela erabiltzailea erasotuz inolako ekintzarik egin gabe. Script gaiztoak sarbidea eman lezake cookie guztietara, saio tokenetara eta nabigatzaileak gordetzen duen eta webgune batekin interaktuatzeko erabiltzen den beste edozein informazio kritikora. Erasotzaileak erabiltzailearen saiora sarbidea izan lezake eta negoziorako kritikoa den informazioa eskuratu. Kasu batzuetan, gainera, haren gaineko kontrola lor liteke. XSS baliatua izan daiteke erakutsitako webguneko edukia baimenik gabe aldatzeko. Ahultasun horretarako CVE-2018-2431 kodea erreserbatu da.

Etiketak: Eguneraketa, SAP, Ahultasuna

Hainbat ahultasun IBMren produktuetan

Argitalpen data: 2018/07/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IBM Content Navigator 2.0.3.8
- IBM Content Navigator 3.0.2
- IBM Content Navigator 3.0.3
- IBM Security Identity Governance and Intelligence (IGI), honako bertsioak: 5.2, 5.2.1, 5.2.2, 5.2.2.1, 5.2.3, 5.2.3.1, 5.2.3.2

Azalpena:

IBMk 3 ahultasun aurkitu ditu, horietako bat larritasun kritikokoa eta beste bi larritasun altukoak. Horiek baliatuz urruneko erasotzaile batek informazio sentikorra eskura lezake, memoriaren baliabideak kontsumitu, segurtasun kudeatzailea desgaitu eta bere pribilegioak igo.

Konponbidea:

IBMk hainbat eguneraketa argitaratu ditu ahultasunak konpontzeko, kaltetutako produktuaren eta bertsioaren arabera.

- IBM Security Identity Governance and Intelligence:
  - 5.2.4.0 bertsiora eguneratzea
- IBM Content Navigator:
  - 2.0.3.8 bertsioaren kasuan 2.0.3 FP8 LA 19 eguneraketa deskargatu Fix Central-en.
  - 3.0.2 bertsioaren kasuan 3.0.2 LA 06 eguneraketa deskargatu Fix Central-en.
  - 3.0.3 bertsioaren kasuan 3.0.3-iFix004 eguneraketa deskargatu FixCentral-en.

Xehetasuna:

- IBM Content Navigator-ek XXE erako ahultasuna dauka XML datuak prozesatzerakoan. Erasotzaile batek informazio sentikorra eskura lezake edo memoriako baliabideak kontsumitu. Ahultasun horretarako CVE-2018-1364 identifikatzailea erreserbatu da.
- IBM J9 VMren klaseen egiaztatzaileak duen akats batek eragin dezake kode ez fidagarri batek segurtasun kudeatzailea desgaitzea eta bere pribilegioak igotzea. Ahultasun horretarako CVE-2017-1376 identifikatzailea erreserbatu da.
- IBM Security Identity Governance Virtual Appliancek XXE erako ahultasuna dauka XML datuak prozesatzerakoan. Urruneko erasotzaile batek informazio sentikorra eskura lezake edo memoriako baliabideak kontsumitu. Ahultasun horretarako CVE-2017-1472 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2018/07/12

Garrantzia: Handia

Kaltetutako baliabideak:

- Cisco Virtualized Packet Core-Single Instance (VPC-SI)
- Cisco Virtualized Packet Core-Distributed Instance (VPC-DI)
- Cisco Ultra Packet Core (UPC)
- IP Phone 6800 Series, Multiplatform Firmware daukana
- IP Phone 7800 Series, Multiplatform Firmware daukana
- IP Phone 8800 Series, Multiplatform Firmware daukana

Azalpena:

Cisco produktuei eragiten dieten hainbat ahultasunen berri eman da. Horiek baliatuz, Cisco IP Phone series 6800, 7800 eta 8800ren web zerbitzarian urruneko kodea exekuta liteke edo StarOS duten produktuetan zerbitzuaren ukapen egoera eragin.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak hemendik deskargatu daitezke: Software Ciscoren deskarga panela.

Xehetasuna:

- Cisco StarOSren IPv4 pakete zatikatuak birmihiztatzeko logikak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek npusim prozesua berrabia lezake bereziki diseinatutako IPv4 pakete bat bidaliz, ondorioz, zerbitzuaren ukapen egoera eraginez. Ahultasun horretarako CVE-2018-0369 identifikatzailea erreserbatu da.
- Sarrera datuen egiaztapen oker bat baliatuz, erasotzaile batek urruneko kodea exekuta lezake Cisco IP Phone, series 6800, 7800 eta 8800ren erabiltzaile interfazetik. Ahultasun horretarako CVE-2018-0341 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun Juniper-en produktuetan

Argitalpen data: 2018/07/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Junos OS, honako bertsioak: 12.1X46, 12.3, 12.3X48, 14.1X53, 15.1X49, 15.1, 15.1F5, 15.1F6, 15.1F7, 16.1, 16.1X65, 17.2X75, 17.3, 17.4
- Junos OS plataformak, MPC7/8/9 edo PTX-FPC3 (FPC-P1, FPC-P2) instalaturik dutenak eta PTX1K 15.1, 15.1F, 16.1, 16.1X65, 16.2, 17.1, 17.2, 17.2X75, 17.3 eta 17.4
- Contrail Service Orchestration 4.0.0 bertsioa
- Junos Space, 18.1R1 bertsioa baino lehenagokoak

Azalpena:

Juniper-ek hainbat segurtasun buletin argitaratu ditu. Horietan zenbait produkturen hainbat ahultasunen berri ematen da, horietako 5 larritasun kritikokoak eta 10 larritasun altukoak.

Konponbidea:

Softwarearen hainbat bertsio, partxeak eta eguneraketak. Hemen daude eskuragarri: https://www.juniper.net/support/downloads/.

Xehetasuna:

Juniper-en zenbait produkturi hainbat ahultasunek eragiten diete: Kaltetutako produktuetan erasotzaile batek ondoko ekintzak egin litzake:

- Erabateko kontrola
- Zerbitzuaren ukapen egoera eragitea.
- Kodearen urrutiko exekuzioa.
- Autentifikazioari ihes egitea.
- Informazioaren zabalkundea baimenik gabe.
- Hainbat zerbitzutara sarbidea baimenik gabe.

Azaldutako ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2018-0024, CVE-2018-10635, CVE-2018-0027, CVE-2018-0030, CVE-2018-0032, CVE-2018-0037, CVE-2017-3145, CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2637, CVE-2018-2663, CVE-2018-2678, CVE-2017-12613, CVE-2017-10198, 2017-10281, CVE-2017-10295, CVE-2017-10345, CVE-2017-10355, CVE-2017-10356, CVE-2017-10388, CVE-2017-15896, CVE-2017-5753, CVE-2017-5715, CVE-2017-5754.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna Linux eta Mac OS Xerako BIG-IP APM bezeroan

Argitalpen data: 2018/07/13

Garrantzia: Handia

Kaltetutako baliabideak:

- BIG-IP (APM), 11.5.1etik 11.5.6ra bitarteko bertsioak, 12.1.0tik 12.1.3ra bitartekoak eta 13.0.0tik 13.1.0ra bitartekoak
- BIG-IP APM bezeroak, 7.1.5etik 7.1.6.1ra bitarteko bertsioak dituztenak
- BIG-IP Edge bezeroak, 7101etik 7150era bitarteko bertsioak dituztenak

Azalpena:

F5ek kritikotasun altuko ahultasun bat aurkitu du. Hori baliatuz, sisteman pribilegiorik ez duen erasotzaile lokal batek informazio sentikorra eskura lezake, datuak manipulatu edo zerbitzua eten.

Konponbidea:

F5ek 7.1.7 eguneraketa argitaratu du BIG-IP APM bezeroetako ahultasuna konpontzeko.

Oraindik ez dago konponbiderik BIG-IP (APM) eta BIG-IP Edge bezeroetarako.

Xehetasuna:

- BIG-IP APM bezeroak duen svpn osagaia pribilegiodun prozesuen bidez exekutatzen da. Hori baliatuz sistemaren erasotzaile lokal batek super erabiltzaile pribilegioak eskura litzake ekipoan. Ahultasun horretarako CVE-2018-5529 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Mugaz kanpoko irakurketa VMware Tools-en

Argitalpen data: 2018/07/16

Garrantzia: Handia

Kaltetutako baliabideak:

- VMware Tools 10.x eta lehenagokoak

Azalpena:

Anurudh ikertzaileak VMwareri larritasun altuko ahultasun baten berri eman dio. Hori baliatuz erasotzaile batek memoriaren mugez kanpoko irakurketa egin lezake.

Konponbidea:

VMwarek tools-en 10.3.0 bertsioa argitaratu du ahultasuna konponduz. Toolsen bertsio berria instalatu behar da Windowsen makina birtual guztietan ahultasuna konpontzeko.

Xehetasuna:

Toolsak instalatuta eta fitxategien partekatzea aktibatuta daukaten Windows makina birtualetan, erasotzaile batek mugez kanpoko irakurketa egin lezake. Hori gertatuz gero ondokoa lor liteke:

- Informaziorako sarbidea baimenik gabe
- Pribilegioak eskalatzea makina birtualetan

Ahultasun horretarako CVE-2018-6969 identifikatzailea erabili da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Eguneraketa kritikoak Oraclen (2018ko uztaila)

Argitalpen data: 2018/07/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Agile Recipe Management for Pharmaceuticals, 9.3.4 bertsioa
- Enterprise Manager Base Platform, 12.1.0.5, 13.2.x bertsioak
- Enterprise Manager for Fusion Middleware, 12.1.0.5, 13.2.x bertsioak
- Enterprise Manager for MySQL Database, 13.2.2.0.0 bertsioa eta lehenagokoak
- Enterprise Manager for Oracle Database, 12.1.0.8, 13.2.2 bertsioak
- Enterprise Manager for Peoplesoft, 13.1.1.1, 13.2.1.1 bertsioak
- Enterprise Manager for Virtualization, 13.2.2, 13.2.3 bertsioak
- Enterprise Manager Ops Center, 12.2.2, 12.3.3 bertsioak
- FMW Platform, 12.2.1.2.0, 12.2.1.3.0 bertsioak
- Hardware Management Pack, 11.3 bertsioa
- Hyperion Data Relationship Management, 11.1.2.4.330 bertsioa
- Hyperion Financial Reporting, 11.1.2 bertsioa
- JD Edwards EnterpriseOne Tools, 9.2 bertsioa
- JD Edwards World Security, A9.3, A9.3.1, A9.4 bertsioak
- MICROS 700 Series Tablet, BIOS 0.00.13ORC baino lehenagoko bertsioak, BIOS 0.01.25ORC baino lehenagoko bertsioak
- MICROS Hyheld Terminal, 2018 bertsioak, yroid 4.4.4 Security Patch Bulletin otsailaren lehena baino lehenagokoak
- MICROS Kitchen Display Controller, BIOS 0.00.16ORC baino lehenagoko bertsioak
- MICROS Lucas, 2.9.5.3, 2.9.5.4, 2.9.5.5, 2.9.5.6 bertsioak
- MICROS Relate CRM Software, 10.8.x, 11.4.x bertsioak
- MICROS Retail-J, 10.2.x, 11.0.x, 12.0.x, 12.1.x, 12.1.1.x, 12.1.2.x, 13.1.x bertsioak
- MICROS Workstation 6, BIOS 1.3.1.0 baino lehenagoko bertsioak, BIOS 1.5.2.0 baino lehenagoko bertsioak, BIOS 2.3.1.0 baino lehenagoko bertsioak
- MICROS XBR, 7.0.2, 7.0.4 bertsioak
- MySQL Client, 5.5.60 bertsioa eta aurrekoak, 5.6.40 eta aurrekoak, 5.7.22 eta aurrekoak, 8.0.11 eta aurrekoak
- MySQL Connectors, 5.3.10 bertsioa eta aurrekoak, 8.0.11 eta aurrekoak
- MySQL Enterprise Monitor, 3.4.7.4297 bertsioa eta aurrekoak, 4.0.4.5235 eta aurrekoak, 8.0.0.8131 eta aurrekoak
- MySQL Server, 5.5.60 bertsioa eta aurrekoak, 5.6.40 eta aurrekoak, 5.7.22 eta aurrekoak, 8.0.11 eta aurrekoak

- MySQL Workbench, 6.3.10 bertsioa eta aurrekoak, 8.0.11 eta aurrekoak
- Oracle Agile Engineering Data Management, 6.1.3, 6.2.0, 6.2.1 bertsioak
- Oracle Agile PLM, 9.3.3, 9.3.4, 9.3.5, 9.3.6 bertsioak
- Oracle Agile PLM MCAD Connector, 3.3, 3.4, 3.5, 3.6 bertsioak
- Oracle Agile Product Lifecycle Management for Process, 6.2.0.0 bertsioa
- Oracle API Gateway, 11.1.2.4.0 bertsioa
- Oracle Application Testing Suite, 10.1 bertsioa
- Oracle AutoVue VueLink Integration, 21.0.0, 21.0.1 bertsioak
- Oracle Banking Corporate Lending, 12.3.0, 12.4.0, 12.5.0, 14.0.0, 14.1.0 bertsioak
- Oracle Banking Payments, 12.2.0, 12.3.0, 12.4.0, 12.5.0, 14.1.0 bertsioak
- Oracle Banking Platform, 2.6.0, 2.6.1, 2.6.2 bertsioak
- Oracle BI Publisher, 11.1.1.7.0, 11.1.1.9.0, 12.2.1.2.0, 12.2.1.3.0 bertsioak
- Oracle Business Process Management Suite, 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0, 12.2.1.3.0 bertsioak
- Oracle Communications Diameter Signaling Router (DSR), 7.x, 8.x bertsioak
- Oracle Communications EAGLE LNP Application Processor, 10.x bertsioa
- Oracle Communications Interactive Session Recorder, 5.x, 6.x bertsioak
- Oracle Communications Calendar Server, 3.x bertsioa
- Oracle Communications Network Charging and Control, 4.4.1.5.0, 5.0.0.1.0, 5.0.0.2.0, 5.0.1.0.0, 5.0.2.0.0 bertsioak
- Oracle Communications Policy Management, 12.x bertsioa
- Oracle Communications Session Border Controller, ECz7.x, ECz8.x bertsioak
- Oracle Communications User Data Repository, 10.x, 12.x bertsioak
- Oracle Database Server, 11.2.0.4, 12.1.0.2, 12.2.0.1, 18.1, 18.2 bertsioak
- Oracle E-Business Suite, 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 bertsioak
- Oracle Endeca Information Discovery Studio, 3.1, 3.2 bertsioak
- Oracle Enterprise Data Quality, 12.2.1.3.0 bertsioa
- Oracle Enterprise Repository, 11.1.1.7.0, 12.1.3.0.0 bertsioak
- Oracle Financial Services Analytical Applications Infrastructure, 7.3.3.x, 8.0.x bertsioak
- Oracle Financial Services Behavior Detection Platform, 8.0.x bertsioa
- Oracle Financial Services Funds Transfer Pricing, 6.1.1, 8.0.x bertsioak
- Oracle Financial Services Hedge Management and IFRS Valuations, 8.0.4, 8.0.5 bertsioak
- Oracle Financial Services Loan Loss Forecasting and Provisioning, 8.0.4, 8.0.5 bertsioak
- Oracle Financial Services Profitability Management, 6.1.1, 8.0.x bertsioak
- Oracle Financial Services Revenue Management and Billing, 2.3.0.2.0, 2.4.0.0.0, 2.4.0.1.0, 2.5.0.1.0, 2.5.0.2.0, 2.5.0.3.0 bertsioak
- Oracle FLEXCUBE Enterprise Limits y Collateral Management, 12.3.0, 14.0.0, 14.1.0 bertsioak
- Oracle FLEXCUBE Investor Servicing, 12.0.4, 12.1.0, 12.3.0, 12.4.0 bertsioak
- Oracle FLEXCUBE Universal Banking, 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0, 14.1.0 bertsioak
- Oracle Fusion Middleware, 12.2.1.2, 12.2.1.3 bertsioak
- Oracle Fusion Middleware MapViewer, 12.2.1.2, 12.2.1.3 bertsioak
- Oracle Global Lifecycle Management OPatchAuto, All bertsioa
- Oracle Hospitality Cruise Fleet Management System, 9.x bertsioa
- Oracle Hospitality Cruise Shipboard Property Management System, 8.x bertsioa
- Oracle Hospitality Gift and Loyalty, 9.0.0 bertsioa
- Oracle Hospitality OPERA 5 Property Services, 5.5.x bertsioa
- Oracle Hospitality Reporting and Analytics, 9.0.0 bertsioa
- Oracle Hospitality Simphony, 2.8, 2.9, 2.10 bertsioak
- Oracle iLearning, 6.2 bertsioa
- Oracle Insurance Policy Administration, 10.0, 10.1, 10.2, 11.0 bertsioak
- Oracle Internet Directory, 11.1.1.9.0 bertsioa
- Oracle Java SE, 6u191, 7u181, 8u172, 10.0.1 bertsioa
- Oracle Java SE Embedded, 8u171 bertsioa
- Oracle JDeveloper, 12.1.3.0.0, 12.2.1.2.0, 12.2.1.3.0 bertsioa
- Oracle JRockit, R28.3.18 bertsioa
- Oracle Outside In Technology, 8.5.3 bertsioa
- Oracle Policy Automation, 10.4.7, 12.1.0, 12.1.1, 12.2.0, 12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7, 12.2.8, 12.2.9, 12.2.10 bertsioak
- Oracle Policy Automation Connector for Siebel, 10.4.6 bertsioa
- Oracle Policy Automation for Mobile Devices, 10.4.7, 12.1.0, 12.1.1, 12.2.0, 12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7, 12.2.8, 12.2.9, 12.2.10 bertsioak
- Oracle Retail Back Office, 14.0, 14.1 bertsioak
- Oracle Retail Bulk Data Integration, 16.0 bertsioa
- Oracle Retail Central Office, 14.0, 14.1 bertsioak
- Oracle Retail Clearance Optimization Engine, 14.0.5 bertsioa
- Oracle Retail Convenience eta Fuel POS Software, 2.1.132 bertsioa
- Oracle Retail Customer Management eta Segmentation Foundation, 16.x, 17.x bertsioak
- Oracle Retail Financial Integration, 13.2.x, 14.0.x, 14.1.x, 15.0.x, 16.0.x bertsioak
- Oracle Retail Integration Bus, 12.0.x, 13.0.x, 13.1.x, 13.2.x, 14.0.0 14.1.0, 14.0.x, 14.1.x, 15.0, 15.0.x, 16.0, 16.0.x bertsioak
- Oracle Retail Order Broker, 5.2, 15.0, 16.0 bertsioak
- Oracle Retail Point-of-Sale, 14.0, 14.1 bertsioak
- Oracle Retail Point-of-Service, 14.0, 14.1 bertsioak
- Oracle Retail Predictive Application Server, 15.0.3 bertsioa
- Oracle Retail Returns Management, 14.0, 14.1 bertsioak
- Oracle Retail Service Backbone, 14.0.x, 14.1.x, 15.0.x, 16.0.x bertsioak
- Oracle Retail Service Layer, 12.0.x, 13.0.x, 13.1.x, 13.2.x, 14.0.x bertsioak
- Oracle Secure Global Desktop, 5.3, 5.4 bertsioak
- Oracle SOA Suite, 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0, 12.2.1.3.0 bertsioak
- Oracle SuperCluster Specific Software, 2.5.0 bertsioa baino lehenagokoak
- Oracle Transportation Management, 6.2, 6.3.7, 6.4.1 bertsioak
- Oracle Tuxedo, 12.1.1, 12.1.3, 12.2.2 bertsioak
- Oracle Utilities Framework, 4.3.x bertsioa
- Oracle Utilities Network Management System, 1.12.x, 2.3.x bertsioak
- Oracle Utilities Work eta Asset Management, 1.9.1.2.12 bertsioak
- Oracle VM VirtualBox, 5.2.16 bertsioa baino lehenagokoak
- Oracle WebCenter Portal, 11.1.1.9.0, 12.2.1.2.0, 12.2.1.3.0 bertsioak
- Oracle WebLogic Server, 10.3.6.0, 12.1.3.0, 12.2.1.2, 12.2.1.3 bertsioak
- OSS Support Tools, 18.3 bertsioa baino lehenagokoak
- PeopleSoft Enterprise CS Financial Aid, 9.0, 9.2 bertsioak
- PeopleSoft Enterprise FIN Install, 9.2 bertsioa
- PeopleSoft Enterprise HCM Human Resources, 9.2 bertsioa
- PeopleSoft Enterprise PeopleTools, 8.55, 8.56 bertsioak
- PeopleSoft HRMS, 9.2 bertsioa
- Primavera P6 Enterprise Project Portfolio Management, 8.4, 15.x, 16.x, 17.x bertsioak
- Primavera Unifier, 16.x, 17.x, 18.x bertsioak
- Siebel Applications, 18.0 bertsioa
- Solaris, 10, 11.2, 11.3 bertsioak

- Solaris Cluster, 3.3, 4.3 bertsioak
- Sun ZFS Storage Appliance Kit (AK), 8.7.20 bertsioa baino lehenagokoak
- Tape Library ACSLS, ACSLS 8.4.0-3 bertsioa baino lehenagokoak

Azalpena:

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

Eragina:

Kaltetutako produktuen araberako partxeak aplikatzea. Eguneraketak deskargatzeko informazioa Oraclek argitaratutako segurtasun buletinean lor daitezke.

Konponbidea:

Eguneraketa horrek 334 ahultasun konpontzen ditu, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna Oracleren loturan dagoen Erreferentzien atalean kontsulta daiteke.

Etiketak: Eguneraketa, Oracle

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2018/07/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco Policy Suite, 18.2.0 eta 18.1.0 baino lehenagoko bertsioak
- Cisco Nexus 9000 Series Fabric Switches in ACI Mode
- Cisco SD-WAN Solution, Release 18.3.0 baino lehenagoko bertsioak:
  - vBond Orchestrator Software
  - vEdge 100 Series Routers
  - vEdge 1000 Series Routers
  - vEdge 2000 Series Routers
  - vEdge 5000 Series Routers
  - vEdge Cloud Router Platform
  - vManage Network Management Software
  - vSmart Controller Software
- Cisco Webex Meetings Suite
- Cisco Webex Meetings Online
- Cisco Webex Meetings Server

Azalpena:

Ciscok hainbat produkturi buruzko 25 ahultasun argitaratu ditu, horietatik 4 larritasun kritikokoak, 9 larritasun altukoak eta 12 larritasun ertainekoak.

Konponbidea:

Ciscok erabiltzaileen eskura jarri ditu hainbat eguneraketa, kaltetutako produktuaren arabera. Hemendik jaits daitezke ahultasunak konpontzen dituzten eguneraketak:

- Software Ciscoren deskarga panela

Xehetasuna:

Honakoak dira larritasun kritikoko ahultasunak:

- Cisco Policy Suiteren Cluster Manager-ek duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek saioa has lezake kaltetutako sistema batean root kontua erabiliz. Kontu horrek erabiltzaile kredentzial estatiko lehenetsiak eta ez-dokumentatuak ditu. Ahultasun horretarako CVE-2018-0375 identifikatzailea erabili da.
- Cisco Policy Suiteren Policy Builder-en datu baseak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile bat zuzenean konekta liteke Policy Builder-en datu basera. Ahultasun honen arrazoia da datu basearen autentifikazio gabezia. Ahultasun horretarako CVE-2018-0374 identifikatzailea erabili da.
- Cisco Policy Suite-ren Open Systems Gateway initiative-ren (OSGi) ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile bat zuzenean konekta liteke OSGi interfazera. Ahultasun honen arrazoia da OSGi zerbitzuaren autentifikazio gabezia. Ahultasun horretarako CVE-2018-0377 identifikatzailea erabili da.
- Cisco Policy Suiteren Policy Builder-en interfazeak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile bat Policy Builder-en interfazera konekta liteke. Ahultasun honen arrazoia da Policy Builder-en interfazearen autentifikazio gabezia. Ahultasun horretarako CVE-2018-0376 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun Jenkins-en

Argitalpen data: 2018/07/19

Garrantzia: Handia

Kaltetutako baliabideak:

Jenkinsen 2.133 bertsioa baino lehenagoko guztiak eta Jenkins LTSren 2.121.2 bertsioa baino lehenagoko guztiak.

Azalpena:

Jenkins proiektuen automatizazio eta hedatze softwarean dauden hainbat ahultasunen berri eman da. Urruneko erasotzaile batek ahultasun horiek balia litzake fitxategi arbitrarioak irakurtzeko, konfigurazioak berrezartzeko, egiten ari diren lanak eteteko edo aplikazioan XSS erako ahultasun bat eragiteko.

Konponbidea:

Jenkinsen 2.133 eta Jenkins TLSren 2.121.2 bertsioetara eguneratzea gomendatzen da.

Xehetasuna:

Kritikotasun altuko ondoko ahultasunak argitaratu dira:

- SECURITY-897: Ahultasun hau baliatuz autentifikatu gabeko erabiltzaileek asmo gaiztoz sortutako saio hasierarako kredentzialak erabil litzakete, eta horren bitartez eragin lezakete Jenkinsek config.xml fitxategia mugitzea Jenkinsen hasierako direktoriotik. Konfigurazio fitxategi honek Jenkinsen oinarrizko konfigurazioa dauka, segurtasun alderdiak barne. Jenkins fitxategi hori gabe abiatzen bada, heredatutako balio lehenetsietara itzuliko da eta erabiltzaile anonimoei administratzaile sarbidea emango die.
- SECURITY-914: Jenkinsek erabiltzen duen Stapler-en web frameworkean fitxategien irakurketa arbitrario erako ahultasun bat aurkitu da. Horrek autentifikatu gabeko erabiltzaileei ahalbidetuko lieke HTTP eskaera manipulatuak bidaltzea eta Jenkinsen prozesuak sarbidea duen Jenkinsen nagusi sistemako edozein fitxategitako edukia eskuratzea.

Kritikotasun ertaineko beste ahultasun batzuk ere argitaratu dira, honako identifikatzaile hauekin: SECURITY-891, SECURITY-892, SECURITY-944, SECURITY-925 eta SECURITY-390.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Apache Tomcat-en

Argitalpen data: 2018/07/24

Garrantzia: Handia

Kaltetutako baliabideak:

- Apache Tomcat, 9.0.0.M9tik 9.0.9ra bitarteko bertsioak
- Apache Tomcat, 8.5.0tik 8.5.31ra bitarteko bertsioak
- Apache Tomcat, 8.0.0.RC1etik 8.0.51ra bitarteko bertsioak
- Apache Tomcat, 7.0.28tik 7.0.86ra bitarteko bertsioak

Azalpena:

Apache Software Foundationek segurtasun eguneraketa bat argitaratu du hainbat ahultasun konpontzeko. Horiek baliatuz urruneko erasotzaile batek zerbitzuaren ukapenak eragin litzake Apache Tomcat zerbitzarian edo bertatik informazio konfidentziala eskuratu lezake.

Konponbidea:

Eskuragarri dauden 9.0.10, 8.5.32, 8.0.52 eta 7.0.90 azken bertsioetara eguneratzea gomendatzen da.

Xehetasuna:

Aurkitutako ahultasunen artean karaktere osagarriak dituen UTF-8 deskodifikazioaren erabilera okerra ere badago. Horrek deskodegailuan begizta infinitu bat eragin dezake, eta ondorioz zerbitzuaren ukapen egoera sortu. Ahultasun horretarako CVE-2018-1336 identifikatzailea erabili da.

Gainera, aurkitutako beste ahultasunak erabiltzailearen saioen berrerabilpena ahalbidetu lezake, indarrean dauden konexioen itxieren segimenduan akats bat baitago. Ahultasun horretarako CVE-2018-1337 identifikatzailea erabili da.

Etiketak: Eguneraketa, Apache, Ahultasuna

Hainbat ahultasun Mbed TLS-n

Argitalpen data: 2018/07/27

Garrantzia: Handia

Kaltetutako baliabideak:

Mbed TLS, 1.2 eta goragoko bertsioak eta 2.1, 2.7 eta goragokoak.

Azalpena:

Mbed TLSk hainbat ahultasunen berri eman du. Horiek baliatuz erasotzaile batek testu laua berreskura lezake, urrunetik CBCn oinarritutako zifratu bat erabiltzen denean.

Konponbidea:

2.12.0, 2.7.5 edo 2.1.14 edo berriagoetara eguneratzea aholkatzen da.

Xehetasuna:

CBCn oinarritutako zifratu bat erabiltzen denean, posible da urruneko erasotzaile batek partzialki berreskuratzea formaturik gabeko testua. Horretarako erasotzaileak sareko trafikoa harrapatu eta injektatzeko gaitasuna izan behar du, eta TLS erabiltzekotan testu berdinarekin hainbat saio hasteko gai izan. DTLSren kasuan, aldiz, saio batekin aski litzateke.

Posible da tenporizazioaren edo cachearen alboko kanalak erabiltzen dituzten mezuetatik formaturik gabeko testua partzialki eskuratzea. Ahultasun horietarako CVE-2018-0497 eta CVE-2018-0498 identifikatzaileak erabili dira.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna