2020ko urtarrilaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun Cisco DCNM produktuetan

Argitalpen data: 2020/01/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Cisco Data Center Network Manager (DCNM), Microsoft Windows, Linux eta gailu birtualen plataformetarako 11.3(1) baino lehenagoko bertsioak.

Azalpena:

Hainbat ahultasun aurkitu dira Cisco produktuetan, 1 larritasun kritikokoa eta 3 larritasun altukoak. Horiek baliatuz urruneko erasotzaile batek ekintza arbitrarioak egin litzake administratzaile baimenekin, SQL komandoak exekutatu, direktorioko jauzi erako erasoak egin edo komandoak injektatu sistema eragilean.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Cisco Softwareren deskargen paneletik deskarga daitezke.

Xehetasuna:

Larritasun kritikoko ahultasunak honakoak dira:

- Zifratze gako estatikoa endopoint REST API eta endpoint SOAP APIren instalazio ezberdinen artean partekatzen da. Hori baliatuz autentifikatu gabeko urruneko erasotzaile batek autentifikazioa saihets lezake kaltetutako gailuan, gako estatiko hori erabiliz saio baliagarri baten token bat sortzeko. Ahultasun horietarako CVE-2019-15975 eta CVE-2019-15976 identifikatzaileak erreserbatu dira.
- Cisco DCNMren webean oinarritutako kudeaketaren interfazean kredentzial estatikoak erabiltzen direla baliatuz, autentifikatu gabeko urruneko erasotzaile batek kredentzial estatiko horiek erabil litzake web interfazean autentifikatzeko eta gailu kaltetu baten informazio konfidentziala eskuratzeko. Informazio hori erabil liteke sistemaren aurka beste eraso batzuk egiteko. Ahultasun horretarako CVE-2019-15977 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako, larritasun altukoak, ondoko identifikatzaileak erreserbatu dira: CVE-2019-15984, CVE-2019-15985, CVE-2019-15980, CVE-2019-15981, CVE-2019-15982, CVE-2019-15978 eta CVE-2019-15979.

Etiketak: Eguneraketa, Cisco, Ahultasuna

SQL injekzio erako ahultasuna phpMyAdmin-en

Argitalpen data: 2020/01/08

Garrantzia: Altua

Kaltetutako baliabideak:

- phpMyAdmin, 4.9.4 baino lehenagoko 4.x bertsioen adarra,
- phpMyAdmin, 5.0.0 bertsioa.

Azalpena:

CSW Research Labs-ek kritikotasun altuko ahultasun bat aurkitu du, phpMyAdmin-en hainbat bertsiori eragiten diena. Erasotzaile batek SQL injekzio bat egin lezake.

Konponbidea:

- 4.x de phpMyAdmin adarraren bertsioak:

    - 4.8 eta 4.9 bertsioen kasuan, 4.9.4 bertsiora edo goragoko batera eguneratzea.
    - Bertsio zaharragoen kasuan, segurtasun partxe hau aplikatzea.
- phpMyAdmin-en 5.x adarraren bertsioen kasuan, 5.0.1 bertsiora edo berriago batera eguneratzea.

Xehetasuna:

Ahultasuna erabiltzaile kontuen orrialdean aurkitu da. Erasotzaile batek SQL injekzio bat egin lezake. Ahultasun horretarako CVE-2020-5504 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, PHP, Ahultasuna

Kodearen exekuzio erako ahultasuna e2fsprogs-en

Argitalpen data: 2020/01/08

Garrantzia: Altua

Kaltetutako baliabideak:

E2fsprogs, 1.43.3 - 1.45.4 bertsioak.

Azalpena:

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

Konponbidea:

e2fsprogs 1.45.5 bertsiora eguneratzea.

Xehetasuna:

Asmo gaiztoz kaltetutako fitxategien sistema bat egiaztatzean dagoen mugez kanpoko idazketa erako ahultasun bat baliatuz, erasotzaile batek kodearen exekuzio arbitrarioa egin lezake. Hau seguruenik ez da baliagarria 64 biteko plataformetan, baina 32 biteko bitarretan izan liteke, konpiladoreak pilaren aldagaiak antolatzen dituen moduaren baitan. Ahultasun horretarako CVE-2019-5188 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Linux, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2020/01/09

Garrantzia: Altua

Kaltetutako baliabideak:

- Cisco IOS eta Cisco IOS XE, HTTP Server funtzionaltasuna gaituta daukaten 16.1.1 baino lehenagoko bertsioak.
- Cisco Webex Video Mesh, 2019.09.19.1956m baino lehenagoko bertsioak.

Azalpena:

Larritasun altuko bi ahultasun aurkitu dira Cisco produktuetan. Horiek baliatuz urruneko erasotzaile batek CSRF (Cross-Site Request Forgery) edo komandoen injekzio erako erasoak egin litzake kaltetutako sisteman.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Cisco Softwareren deskarga paneletik deskarga daitezke.

Xehetasuna:

- Cisco IOS eta Cisco IOS XE programen web erabiltzailearen interfazean aurkitutako CSRF erako ahultasun bat baliatuz, autentifikatu gabeko erasotzaile batek xede den erabiltzailearen pribilegio mailarekin ekintza arbitrarioak egin litzake kaltetutako sisteman. Ahultasun horretarako CVE-2019-16009 identifikatzailea erreserbatu da.
- Cisco Webex Video Mesh-en webean oinarritutako kudeaketaren interfazeak duen ahultasun bat baliatuz, urruneko erasotzaile autentifikatu batek komando arbitrarioak exekuta litzake alboko Linux sistema eragilean root pribilegioekin xede den nodoan. Ahultasun horretarako CVE-2019-16005 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun Juniper produktuetan

Argitalpen data: 2020/01/09

Garrantzia: Altua

Kaltetutako baliabideak:

- Junos OS:
    - 15.1, 15.1R7-S6 baino lehenagoko bertsioak;
    - 15.1X49, 15.1X49-D200 baino lehenagoko bertsioak;
    - 15.1X53, 15.1X53-D592 baino lehenagoko bertsioak;
    - 16.1, 16.1R7-S6 baino lehenagoko bertsioak;

    - 16.2, 16.2R2-S11 baino lehenagoko bertsioak;
    - 17.1, 17.1R2-S11 eta 17.1R3-S1 baino lehenagoko bertsioak;
    - 17.2, 17.2R2-S8 eta 17.2R3-S3 baino lehenagoko bertsioak;
    - 17.3, 17.3R3-S6 baino lehenagoko bertsioak;
    - 17.4, 17.4R2-S7 eta 17.4R3 baino lehenagoko bertsioak;
    - 18.1, 18.1R3-S8 baino lehenagoko bertsioak;
    - 18.2, 18.2R3-S2 baino lehenagoko bertsioak;
    - 18.2X75, 18.2X75-D60 baino lehenagoko bertsioak;
    - 18.3, bertsio hauek baino lehenagokoak: 18.3R1-S6, 18.3R2-S2, 18.3R3;
    - 18.4, bertsio hauek baino lehenagokoak: 18.4R1-S5, 18.4R2-S3, 18.4R3;
    - 19.1, 19.1R1-S3 eta 19.1R2 baino lehenagoko bertsioak;
    - 19.2, 19.2R1-S3 eta 19.2R2 baino lehenagoko bertsioak.
- Junos OS Evolved, 19.3R1 baino lehenagoko bertsioak;
- Juniper Networks Junos OS:
-
    - 16.1, 16.1R7-S6 baino lehenagoko bertsioak;
    - 16.1, 16.1X70-D10 eta ondorengo bertsioak;
    - 16.2, 16.2R2-S11 baino lehenagoko bertsioak;
    - 17.1, 17.1R2-S11 eta 17.1R3-S1 baino lehenagoko bertsioak;
    - 17.2, bertsio hauek baino lehenagokoak: 17.2R1-S9, 17.2R2-S8, 17.2R3-S3;
    - 17.3, 17.3R3-S6 baino lehenagoko bertsioak;
    - 17.4, 17.4R2-S9 eta 17.4R3 baino lehenagoko bertsioak;
    - 18.1, 18.1R3-S7 baino lehenagoko bertsioak;
    - 18.2, 18.2R3-S2 baino lehenagoko bertsioak;
    - 18.2X75, 18.2X75-D50 eta 18.2X75-D410 baino lehenagoko bertsioak;
    - 18.3, bertsio hauek baino lehenagokoak: 18.3R1-S6, 18.3R2-S2, 18.3R3;
    - 18.4, 18.4R2-S2 eta 18.4R3 baino lehenagoko bertsioak;
    - 19.1, 19.1R1-S3 eta 19.1R2 baino lehenagoko bertsioak;
    - 19.2, 19.2R1-S2 eta 19.2R2 baino lehenagoko bertsioak.
    - 12.3, 12.3R12-S15 baino lehenagoko bertsioak;
    - 12.3X48, 12.3X48-D86 eta 12.3X48-D90 baino lehenagoko bertsioak SRX Series-en;
    - 14.1X53 , 14.1X53-D51 baino lehenagoko bertsioak EX eta QFX Series-en;
    - 15.1F6, 15.1F6-S13 baino lehenagoko bertsioak;
    - 15.1, 15.1R7-S5 baino lehenagoko bertsioak;
    - 15.1X49, 15.1X49-D181 eta 15.1X49-D190 baino lehenagoko bertsioak SRX Series-en;
    - 15.1X53, 15.1X53-D238 baino lehenagoko bertsioak QFX5200/QFX5110 Series-en;
    - 15.1X53, 15.1X53-D592 baino lehenagoko bertsioak EX2300/EX3400 Series-en;
    - 16.1, 16.1R4-S13 eta 16.1R7-S5 baino lehenagoko bertsioak;
    - 16.2, 16.2R2-S10 baino lehenagoko bertsioak;
    - 17.1, 17.1R2-S11 eta 17.1R3-S1 baino lehenagoko bertsioak;
    - 17.2, 17.2R1-S9 eta 17.2R3-S2 baino lehenagoko bertsioak;
    - 17.3, 17.3R2-S5 eta 17.3R3-S5 baino lehenagoko bertsioak;
    - 17.4, 17.4R2-S6 eta 17.4R3 baino lehenagoko bertsioak;
    - 18.1, 18.1R3-S7 baino lehenagoko bertsioak;
    - 18.2, 18.2R2-S5 eta 18.2R3 baino lehenagoko bertsioak;
    - 18.3, bertsio hauek baino lehenagokoak: 18.3R1-S6, 18.3R2-S1, 18.3R3;
    - 18.4, 18.4R1-S5 eta 18.4R2 baino lehenagoko bertsioak;
    - 19.1, 19.1R1-S2 eta 19.1R2 baino lehenagoko bertsioak.
- Juniper Networks Junos OS duen MX Series:
    - 17.2, 17.2R2-S6, 17.2R3 eta ondoreneko bertsioak;
    - 17.3, 17.3R2-S5 eta 17.3R3-S5 baino lehenagoko bertsioak;
    - 17.4, 17.4R2-S7,17.4R3 baino lehenagoko bertsioak;
    - 18.1, 18.1R3-S6 baino lehenagoko bertsioak;
    - 18.2, 18.2R3-S2 baino lehenagoko bertsioak;
    - 18.2X75, 18.2X75-D51 eta 18.2X75-D60 baino lehenagoko bertsioak;
    - 18.3, 18.3R3 baino lehenagoko bertsioak;
    - 18.4, 18.4R2 baino lehenagoko bertsioak;
    - 19.1, 19.1R1-S3 eta 19.1R2 baino lehenagoko bertsioak;
    - 19.2, 19.2R1-S2 eta 19.2R2 baino lehenagoko bertsioak.

Descripción:

Juniper produktuek dituzten hainbat ahultasun argitaratu dira. Horiek baliatuz erasotzaile batek hainbat ekintza egin litzake: root modura komandoak exekutatu, zerbitzuaren ukapena eragin, J-Web saioa bahitu administrazio ekintzak egiteko, edo gailuaren ustekabeko itxiera eta bere berrabiatzea eragin.

Solución:

Kaltetutako produktuak Juniper-en deskargen zentrotik eguneratzea.

Detalle:

- Juniper Network-en JDHCPD modua baliatuz, erasotzaile batek bereziki diseinatutako paketeak bidal litzake root modura komando arbitrarioak exekutatzeko xede den gailuan, edo JDHCPD prozesuaren kodearen exekuzioa bere kargu har lezake. Ahultasun horretarako CVE-2020-1602, CVE-2020-1605 eta CVE-2020-1609 identifikatzaileak erreserbatu dira.
- Bezeroek bidalitako IPv6ren pakete berezien erabilera okerrak eragin lezake bezeroaren gailuetako IPv6ren trafikoa galtzea, eta gailuaren barnean memoriaren galera eragitea. Horrek kernel-aren (vmcore) blokeatzea ekar lezake zerbitzuaren ukapen egoera (DoS) sortuz. Ahultasun horretarako CVE-2020-1603 identifikatzailea erreserbatu da.
- J-Web-en Cross-Site Scripting (XSS) erako erasoen aurkako babes ez-nahikoa baliatuz, urruneko erasotzaile batek web edo HTML komandoen sekuentziak injekta litzake, xede den erabiltzailearen J-Web-en saioa bahitu edo Junos gailuan ekintza administratzaileak egin beste erabiltzaile bat balitz bezala. Ahultasun horretarako CVE-2020-1607 identifikatzailea erreserbatu da.
- Broadband Edge (BBE) zerbitzurako konfiguratuta badago, MX serieko gailu baten core-aren interfazean MPLS edo IPv6 pakete berezi bat jasotzean, vmcore-ren ustekabeko itxiera gerta liteke, gailua berrabiaraziz. Ahultasun horretarako CVE-2020-1608 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Microsoften 2020ko urtarrileko segurtasun buletina

Argitalpen data: 2020/01/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows;
- Internet Explorer;
- Microsoft Office, Microsoft Office Services y Web Apps;
- ASP.NET Core;
- .NET Core;
- .NET Framework;
- OneDrive para Android;
- Microsoft Dynamics;

Azalpena:

Segurtasun eguneraketei buruzko Microsoften urtarrileko argitalpenean 50 ahultasun jaso dira, 8 kritiko gisa sailkatu dira eta 42 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, Nabigatzailea, Ahultasuna, Windows

---

SAP-en 2020ko urtarrileko segurtasun eguneraketa

Argitalpen data: 2020/01/15

Garrantzia: Ertaina

Kaltetutako baliabideak:

- SAP Process Integration - Rest Adapter (SAP_XIAF), honako bertsioak: 7.31, 7.40, 7.50;
- SAP NetWeaver Internet Communication Manager, honako bertsioak:
  - KRNL32NUC y KRNL32UC 7.21, 7.21EXT, 7.22 eta 7.22EXT;
  - KRNL64NUC y KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT eta 7.49;
  - KERNEL 7.21, 7.22, 7.49 eta 7.53;
- RTCISM, 100 bertsioa;
- SAP Disclosure Management, 10.1 bertsioa;
- Automated Note Search Tool (SAP Basis), honako bertsioak: 7.0, 7.01,7.02, 7.31, 7.4, 7.5, 7.51, 7.52, 7.53 eta 7.54;
- SAP UI, honako bertsioak: 7.5, 7.51, 7.52, 7.53 eta 7.54;
- SAP UI 700, 2.0 bertsioa;
- SAP Leasing, honako bertsioak:
  - (SAP_Appl) 6.18;
  - (EA_Appl) 6.0, 6.02, 6.03, 6.04, 6.05, 6.06, 6.16 eta 6.17;

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:

APek segurtasun partxeei buruz argitaratzen duen hileroko komunikatuan 6 segurtasun ohar eta eguneraketa bat eman ditu ezagutzera. Eguneraketa eta oharren artetik 4 larritasun ertainekoak dira eta beste oharretako bat larritasun baxukoa.

Argitaratutako ahultasun motak honako hauek dira:

- Baimenaren egiaztapen gabeziako 3 ahultasun;
- edukiaren ordezte erako ahultasun bat;
- DoS (Denial of Service) erako ahultasun bat;
- XSS (Cross-Site Scripting) erako ahultasun bat;
- beste era bateko ahultasun bat.

Ahultasun horietarako honako identifikatzaileak erreserbatu dira: CVE-2020-6305, CVE-2020-6304, CVE-2020-6303, CVE-2020-6307, CVE-2019-0388 eta CVE-2020-6306.

Etiketak: Eguneraketa, SAP, Ahultasuna

Ahultasuna VMware Tools-en

Argitalpen data: 2020/01/15

Garrantzia: Altua

Kaltetutako baliabideak:

- VMware Tools, Windowserako 10.x.y bertsioa.

Azalpena:

Kritikotasun altuko ahultasunen baten berri eman da. Erasotzaile lokal batek pribilegioen eskalatzea egin lezake sisteman.

Konponbidea:

- VMware Tools 11.0.0 bertsiora edo berriagoetara eguneratzea gomendatzen da.
- Eguneratzea posible ez bada, ahultasuna baliatzea eragotz daiteke VMware-ren jarraibide hauek betez.

Xehetasuna:

Windowserako VMware Tools-en konponketaren eragiketak lasterketa baldintza bat dauka. Erasotzaile batek, gonbidatutako makina birtualean, pribilegioak eskala litzake Windowsen makina birtual batean. Ahultasun horretarako CVE-2020-3941 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Birtualizazioa, VMware, Ahultasuna

Eguneraketa kritikoak Oracle-n (2020ko urtarrila)

Argitalpen data: 2020/01/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Enterprise Manager Base Platform, 12.1.0.5, 13.2.0.0, 13.3.0.0 bertsioak;
- Enterprise Manager for Fusion Middleware, 13.2.0.0, 13.3.0.0 bertsioak;
- Enterprise Manager for Oracle Database, 12.1.0.5, 13.2.0.0, 13.3.0.0 bertsioak;
- Enterprise Manager Ops Center, 12.3.3, 12.4.0 bertsioak;
- Hyperion Financial Close Management, 11.1.2.4 bertsioa;
- Hyperion Planning, 11.1.2.4 bertsioa;
- Identity Manager, 11.1.2.3.0, 12.2.1.3.0 bertsioak;
- Instantis EnterpriseTrack, 17.1, 17.2, 17.3 bertsioak;
- JD Edwards EnterpriseOne Orchestrator, 9.2 bertsioa;
- JD Edwards EnterpriseOne Tools, 9.2 bertsioa;
- MySQL Client, 5.6.46 eta lehenagoko bertsioak, 5.7.28 eta lehenagokoak, 8.0.18 eta lehenagokoak;
- MySQL Cluster, 7.3.27 bertsioa eta aurrekoak, 7.4.25 bertsioa eta aurrekoak, 7.5.15 bertsioa eta aurrekoak, 7.6.12 bertsioa eta aurrekoak;
- MySQL Connectors, 5.3.13 eta lehenagoko bertsioak, eta 8.0.18 eta lehenagokoak;
- MySQL Enterprise Backup, 3.12.4 eta lehenagoko bertsioak, eta 4.1.3 eta lehenagokoak;
- MySQL Server, 5.6.46 eta lehenagoko bertsioak, 5.7.28 eta lehenagokoak, 8.0.18 eta lehenagokoak;
- MySQL Workbench, 8.0.18 eta lehenagoko bertsioak;
- Oracle Agile Engineering Data Management, 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 Framework, 9.3.3 bertsioa;
- Oracle Agile PLM MCAD Connector, 3.4, 3.5, 3.6 bertsioak;
- Oracle Application Testing Suite, 12.5.0.3, 13.1.0.1, 13.2.0.1, 13.3.0.1 bertsioak;
- Oracle AutoVue, 12.0.2 bertsioa;
- Oracle Banking Corporate Lending, 12.3.0-12.4.0, 14.0.0-14.3.0 bertsioak;
- Oracle Banking Payments, 14.1.0-14.3.0 bertsioak;
- Oracle Big Data Discovery, 1.6 bertsioa;
- Oracle Business Intelligence Enterprise Edition, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Clinical, 5.2 bertsioa;
- Oracle Coherence, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 bertsioa;
- Oracle Communications Design Studio, 7.3.4.3.0, 7.3.5.5.0, 7.4.0.4.0, 7.4.1.1.0 bertsioak;
- Oracle Communications Diameter Signaling Router (DSR), 8.0, 8.1, 8.2, 8.3, 8.4 bertsioak;
- Oracle Communications Instant Messaging Server, 10.0.1.3.0 bertsioa;
- Oracle Communications Interactive Session Recorder, 6.0, 6.1, 6.2, 6.3 bertsioak;
- Oracle Communications IP Service Activator, 7.3.4, 7.4.0 bertsioak;
- Oracle Communications Session Border Controller, 7.4, 8.0, 8.1, 8.2, 8.3 bertsioak;
- Oracle Communications Session Border Controller, 7.4, 8.0, 8.1, 8.2, 8.3 bertsioak;
- Oracle Communications Subscriber-Aware Load Balancer, 7.3, 8.1, 8.3 bertsioak;
- Oracle Communications Unified Inventory Management, 7.3, 7.4 bertsioak;
- Oracle Communications Unified Session Manager, 7.3.5, 8.2.5 bertsioak;
- Oracle Database Server, 11.2.0.4, 12.1.0.2, 12.1.0.11, 12.2.0.1, 18c, 19c, 29, 212.2.0.1 bertsioak;
- Oracle Demantra Demand Management, 12.2.4, 12.2.4.1, 12.2.5, 12.2.5.1 bertsioak;
- Oracle E-Business Suite, 12.1.1-12.1.3, 12.2.3-12.2.9 bertsioak;Oracle Endeca Information Discovery Integrator, 3.2.0 bertsioa;
- Oracle Endeca Information Discovery Studio, 3.2.0 bertsioa;
- Oracle Enterprise Communications Broker, PCz3.0, PCz3.1, PCz3.2 bertsioak;
- Oracle Enterprise Repository, 12.1.3.0.0 bertsioa;
- Oracle Enterprise Session Border Controller, 7.5, 8.0, 8.1, 8.2, 8.3 bertsioak;
- Oracle Financial Services Analytical Applications Infrastructure, 7.3.3-7.3.5, 8.0.0-8.0.8 bertsioak;
- Oracle Financial Services Funds Transfer Pricing, 8.0.2-8.0.7 bertsioak;
- Oracle Financial Services Revenue Management and Billing, 2.7.0.0, 2.7.0.1, 2.8.0.0 bertsioak;
- Oracle FLEXCUBE Investor Servicing, 12.1.0-12.4.0, 14.0.0-14.1.0 bertsioak;
- Oracle FLEXCUBE Universal Banking, 12.0.1-12.4.0, 14.0.0-14.3.0 bertsioak;
- Oracle GraalVM Enterprise Edition, 19.3.0.2 bertsioa;
- Oracle Health Sciences Data Management Workbench, 2.4, 2.5 bertsioak;
- Oracle Healthcare Master Person Index, 3.0 bertsioa;
- Oracle Hospitality Cruise Materials Management, 7.30.567 bertsioa;
- Oracle Hospitality Guest Access, 4.2 bertsioa;
- Oracle Hospitality OPERA 5, 5.5, 5.6 bertsioak;
- Oracle Hospitality Suites Management, 3.7, 3.8 bertsioak;

- Oracle HTTP Server, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0 bertsioak;
- Oracle iLearning, 6.1 bertsioa;
- Oracle Java SE, 7u241, 8u231, 8u241, 11.0.5, 13.0.1 bertsioak;
- Oracle Java SE Embedded, 8u231 bertsioa;
- Oracle Outside In Technology, 8.5.4 bertsioa;
- Oracle Real-Time Scheduler, 2.3.0.1-2.3.0.3 bertsioak;
- Oracle Reports Developer, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Retail Assortment Planning, 15.0.3, 16.0.3 bertsioak;
- Oracle Retail Clearance Optimization Engine, 13.4, 14.0, 14.0.3, 14.0.5 bertsioak;
- Oracle Retail Customer Management y Segmentation Foundation, 16.0, 17.0, 18.0 bertsioak;
- Oracle Retail Markdown Optimization, 13.4, 13.4.4 bertsioak;
- Oracle Retail Order Broker, 5.2, 15.0, 16.0, 18.0 bertsioak;
- Oracle Retail Predictive Application Server, 15.0.3, 16.0.3 bertsioak;
- Oracle Retail Sales Audit, 15.0.3.16.0.2 bertsioa;
- Oracle Secure Global Desktop, 5.4, 5.5 bertsioak;
- Oracle Security Service, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0 bertsioak;
- Oracle Solaris, 10, 11 bertsioak;
- Oracle Tuxedo, 12.1.1.0.0, 12.1.3.0.0 bertsioak;
- Oracle Utilities Framework, 4.2.0.2-4.2.0.3, 4.3.0.1-4.3.0.4 bertsioak;
- Oracle Utilities Mobile Workforce Management, 2.3.0.1-2.3.0.3 bertsioak;
- Oracle Utilities Work eta Asset Management (v1), 1.9.1.2 bertsioa;
- SPARCerako Oracle VM Server, 3.6 bertsioa;
- Oracle VM VirtualBox, 5.2.36 baino lehenagoko bertsioak, 6.0.16 baino lehenagokoak, 6.1.2 baino lehenagokoak;
- Oracle WebCenter Sites, 12.2.1.3.0 bertsioa;
- Oracle WebLogic Server, 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- PeopleSoft Enterprise CC Common Application Objects, 9.1, 9.2 bertsioak;
- PeopleSoft Enterprise HCM Human Resources, 9.2 bertsioa;
- PeopleSoft Enterprise PeopleTools, 8.56, 8.57, 8.58 bertsioak;
- PeopleSoft PeopleTools, 8.56, 8.57 bertsioak;
- Primavera Gateway, 15.2.18, 16.2.11, 17.12.6, 18.8.8.1 bertsioak;
- Primavera P6 Enterprise Project Portfolio Management, 15.1.0.0-15.2.18.7, 16.1.0.0-16.2.19.0, 17.1.0.0-17.12.16.0, 18.1.0.0-18.8.16.0, 19.12.0.0, 20.1.0.0 bertsioak;
- Primavera Unifier, 16.1, 16.2, 17.7-17.12, 18.8, 19.12 bertsioak;
- Siebel Applications, 19.10 eta lehenagoko bertsioak;
- Sun ZFS Storage Appliance Kit, 8.8.6 bertsioa;
- Tape Library ACSLS, 8.5, 8.5.1 bertsioak.

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 255 ahultasun konpontzen ditu guztira (334 partxerekin), horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna Erreferentziak atalean dagoen Oracleren loturan kontsulta daiteke.

Etiketak: Eguneraketa, Ahultasuna, Oracle

Ahultasuna Intel-en Windows-erako VTune Amplifier-en

Argitalpen data: 2020/01/15

Garrantzia: Altua

Kaltetutako baliabideak:

Windowserako Intel VTune Amplifier, 8. eguneraketa baino lehenagoko bertsioak.

Azalpena:

Intelek kritikotasun altuko ahultasun bat aurkitu du. Erasotzaile lokal batek pribilegioen eskalatzea egin lezake sisteman.

Konponbidea:

Windowserako Intel VTune Amplifier-en 8. eguneraketa edo berriagoa aplikatzea.

Xehetasuna:

Windowserako Intel VTune Amplifier-erako driverrak duen sarbide kontrol desegokia baliatuz, erasotzaile lokal batek pribilegioen eskalatzea egin lezake sisteman. Ahultasun horretarako CVE-2019-14613 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna HPEren Superdome Flex Server-en

Argitalpen data: 2020/01/16

Garrantzia: Altua

Kaltetutako baliabideak:

HPE Superdome Flex Server, 3.20.186 eta lehenagoko bertsioak.

Azalpena:

HPEk kritikotasun altuko ahultasun bat aurkitu du, bere Flex Superdome zerbitzariari eragiten diona. Administratzaile pribilegioak lituzkeen urruneko erasotzaile batek informazioa heda lezake.

Konponbidea:

Gailuaren firmware-a 3.20.206. bertsiora edo berriago batera eguneratzea.

Xehetasuna:

Ahultasunaren jatorria administratzaile komandoen sarreraren egiaztatze desegokia da. Administratzaile pribilegioak lituzkeen urruneko erasotzaile batek segurtasun murrizpenak saihets litzake eta informazioa hedatu. Ahultasun horretarako CVE-2019-11998 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, HP, Ahultasuna

XSS erako ahultasuna Moodle-n gorderik

Argitalpen data: 2020/01/20

Garrantzia: Altua

Kaltetutako baliabideak:

Moodle, 3.8 bertsioa.

Azalpena:

Cid da Costa ikertzaileak kritikotasun altuko ahultasun bat aurkitu du Moodlen. Urruneko erasotzaile batek kode arbitrarioa exekuta lezake sisteman.

Konponbidea:

- Moodle 3.8.1 bertsiora eguneratzea.
- Prebentzio neurri modura, Moodlek gomendatzen du mezularitza sistema desgaitzea eguneraketa aplikatu arte.

Xehetasuna:

Ahultasunaren jatorria da garbiketa desegoki bat elkarrizketen laburpena eguneratu baino lehen. Erasotzaile batek gordetako Cross-site-scripting (XSS) erako eraso bat egin lezake eta kode arbitrarioa exekutatu. Ahultasun horretarako CVE-2020-1691 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Zerbitzuaren ukapen egoera Dell EMCren Unity eta Unity XT familietan

Argitalpen data: 2020/01/21

Garrantzia: Altua

Kaltetutako baliabideak:

- Dell EMC Unity eta Unity XT Operating Environment (OE), 5.0.2.0.5.009 baino lehenagoko bertsioak;
- Dell EMC Unity VSA Operating Environment (OE), 5.0.2.0.5.009 baino lehenagoko bertsioak.

Azalpena:

Dell EMCk kritikotasun altuko ahultasun bat aurkitu du. Autentifikaziorik gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake.

Konponbidea:

- Dell EMC Unity eta Dell EMC Unity XT Operating Environment (OE) 5.0.2.0.5.009 bertsiora edo berriagora eguneratzea;
- Dell EMC Unity VSA Operating Environment (OE) 5.0.2.0.5.009 bertsiora edo berriagora eguneratzea.

Xehetasuna:

Ahultasuna NAS zerbitzarian SFTP zerbitzurako erabilitako SSHren inplementazioan datza. Autentifikaziorik gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake. Ahultasun horretarako CVE-2020-5319 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

TLS ziurtagiriaren gako pribatua hedatzea Netgear routerretan

Argitalpen data: 2020/01/23

Garrantzia: Altua

Kaltetutako baliabideak:

Router modelo hauek:

- R8900;
- R9000;
- RAX120;
- XR700.

Azalpena:

Netgear-ek larritasun altuko ohartarazpen bat argitaratu du, TLS ziurtagiriaren gako pribatuaren hedapen erako ahultasun baten berri buruz informatuz.

Konponbidea:

NETGEARek kaltetutako produktu guztientzat ahalik azkarren firmware hotfix-ak argitaratzea aurreikusten du. Ordura arte fabrikatzaileak gomendatzen du NETGEAR Nightawk app-a erabiltzea edo login egitea routerraren web interfazean HTTP (http://routerlogin.com) erabiliz HTTPSren ordez.

Xehetasuna:

Kaltetutako produktuek Ziurtatze Agintaritza (CA) batek sinatutako ziurtagiriak erabiltzen dituzte, bere web interfazera sarbide seguru bat eskaintzeko HTTPSren bidez. Routerraren web interfazera HTTPS bitartez sartzen saiatzean gerta liteke akats mezu bat edo segurtasun ziurtagiriaren ohartarazpen bat agertzea.

Etiketak: SSL/LTS, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2020/01/23

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco FMC Software, kudeaketaren web interfazearen erabiltzaileen autentifikazioa kanpoko LDAP zerbitzari baten bidez egiteko konfiguratuta badago;
- Cisco TelePresence:
  - Integrator C Series;
  - MX Series;
  - SX Series;
  - System EX Series.
- Cisco Webex:
  - Board;
  - DX Series;
  - Room Series.
- Cisco IOS XE SD-WAN Software, 16.11 eta lehenagoko bertsioak;
- Cisco SD-WAN Solution vManage Software, 18.4.1 bertsioa;
- Cisco Smart Software Manager On-Prem, 7-201910 baino lehenagoko bertsioak;
- Cisco IOS XR Software, 6.6.1en ondorengo bertsioak edo 6.6.3, 7.0.2, 7.1.1 edo 7.2.1 baino lehenagokoak.

Azalpena:

12 ahultasun aurkitu dira Cisco produktuetan, bat larritasun kritikokoa eta gainerakoak larritasun altukoak. Horiek baliatuz, LDAPn autentifikazioa saihets liteke, bideetara sarbide ez-kontrolatua lortu, lehenetsitako kredentzialak erabili, pribilegioak eskalatu edo zerbitzuaren ukapen egoera eragin.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Cisco Softwarearen deskarga paneletik deskarga daitezke.

Xehetasuna:

- Larritasun kritikoko ahultasuna baliatuz, autentifikatu gabeko urruneko erasotzaile batek LDAP protokoloaren autentifikazioa saihets lezake, eta ekintza arbitrarioak egin litzake administratzaile pribilegioekin kaltetutako gailuan. Ahultasun horretarako CVE-2019-16028 identifikatzailea erreserbatu da.
- Gainerako ahultasunek, larritasun altukoak, ondoko eraso motak egitea ahalbidetu lezakete:
  - bideetara kontrolatu gabeko sarbidea;
  - lehenetsitako kredentzialen erabilpena;
  - pribilegioen eskalatze lokala;
  - zerbitzuaren ukapena.

Kritikotasun altuko ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2020-3143, CVE-2019-1950, CVE-2020-3115, CVE-2019-16029, CVE-2019-16018, CVE-2019-16019, CVE-2019-16020, CVE-2019-16021, CVE-2019-16022, CVE-2019-16023 eta CVE-2019-16027.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Segurtasun murrizketak saihestea IBMren MQ Appliance-n

Argitalpen data: 2020/01/24

Garrantzia: Altua

Kaltetutako baliabideak:

- IBM MQ Appliance, 8.0 bertsioa;
- IBM MQ Appliance, 9.1 LTS bertsioa;
- IBM MQ Appliance, 9.1 CD bertsioa.

Azalpena:

IBMk kritikotasun altuko ahultasun bat aurkitu du bere MQ Appliance produktuei eragiten diena. Erasotzaile lokal batek segurtasun murrizpenak saihets litzake.

Konponbidea:

- IBM MQ Appliance 8 bertsioa, 8.0.0.14 bertsiora edo berriagora eguneratzea.
- IBM MQ Appliance 9.1 LTS bertsioa, 9.1.0.4 bertsiora edo berriagora eguneratzea.
- IBM MQ Appliance 9.1 CD bertsioa, 9.1.4 bertsiora edo berriagora eguneratzea.

Xehetasuna:

Ahultasunaren jatorria inguruaren aldagaien baliozkotze oker bat da. Erasotzaile lokal batek segurtasun murrizpenak saihets litzake. Ahultasun horretarako CVE-2019-4620 kodea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Bileretara autentifikaziorik gabe sartze erako ahultasuna Cisco Webex-en

Argitalpen data: 2020/01/27

Garrantzia: Altua

Kaltetutako baliabideak:

- Cisco Webex Meetings Suite, 39.11.5 baino lehenagoko bertsioak;
- Cisco Webex Meetings Online, 40.1.3 baino lehenagoko bertsioak.

Azalpena:

Larritasun altuko ahultasun bat aurkitu da Cisco produktuetan. Hori baliatuz, autentifikatu gabeko urruneko erasotzaile bat pasahitzez babestutako bideokonferentzia bidezko bilera batera sar liteke.

Konponbidea:

Aipatutako ahultasuna konpontzen duten eguneraketak Cisco Softwarearen deskarga paneletik deskarga daitezke.

Xehetasuna:

- Cisco Webex Meetings Suite eta Cisco Webex Meetings Online produktuek duten ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile bat pasahitzez babestutako bilera batera sar liteke bileraren pasahitza eman gabe. Konexio saioa Webex-ek iOS edo Androiderako duen aplikazio mugikor batetik egin beharra dago. Ahultasun horretarako CVE-2020-3142 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun IBM produktuetan

Argitalpen data: 2020/01/27

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IBM Security Secret Server, bertsio guztiak;
- IBM WIoTP MessageGateway, 5.0.0.1 bertsioa;
- IBM IoT MessageSight, 5.0.0.0 bertsioa;
- IBM IoT MessageSight, 2.0 bertsioa.

Azalpena:

IBMk hainbat produkturi eragiten dieten bi ahultasun aurkitu ditu, bat larritasun altukoa eta bestea kritikoa. Urruneko erasotzaile batek kode arbitrarioa exekuta lezake sisteman, zerbitzuaren ukapen egoera (DoS) sortu edo informazio sentikorra eskuratu.

Konponbidea:

- IBM Security Secret Server, 10.7 bertsiora edo berriago batera eguneratzea;
- IBM WIoTP MessageGateway, 5.0.0.2 bertsiora eguneratzea;
- IBM MessageSight, 5.0.0.0 bertsiora eguneratzea;
- IBM MessageSight, 2.0.0.2 bertsiora eguneratzea.

Xehetasuna:

- Larritasun kritikoko ahultasunak Watson IoT MessageGateway Server gailuei eragiten die. Gailu horiek ahulak dira bufferraren gainezkatze baten aurrean, akastun HTTP eskaerak kudeatzen dituztenean euren goiburuetan bereziki sortutako edukia badute. Urruneko erasotzaile batek kode arbitrarioa exekuta lezake edo zerbitzuaren ukapen egoera (DoS) sortu. Ahultasun horretarako CVE-2020-4207 identifikatzailea erreserbatu da.

- Kritikotasun altuko ahultasunak Security Secret Server-i eragiten dio. Gailuak ahulak dira birbideratze ireki erako eraso baten aurrean, eta biktima engainatzeko bereziki sortutako webak egin litezke. Urruneko erasotzaile batek informazio sentikorra eskura lezake. Ahultasun horretarako CVE-2019-4631 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

XXE injekzio erako ahultasuna IBM Security Access Manager-en

Argitalpen data: 2020/01/28

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Security Access Manager (ISAM), 9.0 bertsioa.

Azalpena:

IBM X-Force Ethical Hacking Team-eko hainbat ikertzailek *XML External Entity* (XXE) erako larritasun altuko ahultasun bat aurkitu dute IBM Security Access Manager-en.

Konponbidea:

IBM Security Access Manager 9.0.7.1 bertsiora eguneratzea.

Xehetasuna:

IBM Security Access Manager (ISAM) ahula da *XML External Entity* (XXE) erako erasoen aurrean, XML datuak prozesatzen dituenean. Urruneko erasotzaile batek ahultasun hori balia lezake informazio sentikorra agerian uzteko edo memoriaren baliabideak kontsumitzeko. Ahultasun horretarako CVE-2019-4707 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

XSS erako ahultasuna TIBCO Patterns - Search-en

Argitalpen data: 2020/01/29

Garrantzia: Altua

Kaltetutako baliabideak:

TIBCO Patterns - Search, 5.4.0 bertsioa eta lehenagokoak.

Azalpena:

TIBCOk kritikotasun altuko ahultasun bat aurkitu du, TIBCO Patterns - Search produktuari eragiten diona. Urruneko erasotzaile batek sistemaren pribilegio guztiak eskura litzake.

Konponbidea:

TIBCO Patterns - Search 5.5.0 bertsiora edo goragoko batera eguneratzea.

Xehetasuna:

TIBCO Patterns - Search-en erabiltzaile interfazea ahula da Cross-Site Scripting (XSS) erako erasoen aurrean. Urruneko erasotzaile batek sistemaren pribilegio guztiak eskura litzake. Ahultasun horretarako CVE-2019-17388 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Joomla! 3.9.15en segurtasun eguneraketa

Argitalpen data: 2020/01/29

Garrantzia: Txikia

Kaltetutako baliabideak:

Joomla! CMS, 3.0.0tik 3.9.14ra bitarteko bertsioak.

Azalpena:

Joomla!-k bertsio berri bat argitaratu du, nukleoak dituen kritikotasun baxuko hiru ahultasun konpontzen dituena, CSRF eta XSS erakoak.

Solución:

3.9.15 bertsioara eguneratzea.

Xehetasuna:

- Hainbat osagaietako loteen ekintzetan kontrol sinbolikoen gabeziak CSRF (*Cross-Site Request Forgery*) erako ahultasunak eragiten ditu. Ahultasun horretarako CVE-2020-8419 identifikatzailea erabili da.
- *com_templates*-en LESS konpiladorearen barnean CSRF erako erasoak token-ean egiaztatzen ez direnez, era horretako erasoak

gerta litezke. Ahultasun horretarako CVE-2020-8420 identifikatzailea erabili da.
- Erabiltzaile izenen ihes desegokiak XSS (*Cross-Site Scripting*) erako erasoak ahalbidetzen ditu *com_actionlogs*-en. Ahultasun horretarako CVE-2020-8421 identifikatzailea erabili da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Baimentze desegoki erako ahultasuna Dell EMC Isilon OneFS-n

Argitalpen data: 2020/01/30

Garrantzia: Altua

Kaltetutako baliabideak:

Dell EMC Isilon OneFS, honako bertsioak:

- 8.1.2;
- 8.1.0.4;
- 8.1.0.3;
- 8.0.0.7.

Azalpena:

Dell EMC-k kritikotasun altuko ahultasun bat aurkitu du. Hori baliatuz urruneko erasotzaile batek kaltetutako ekipoa arriskuan jar lezake fitxategi murriztuetara sarbidea lortuz.

Konponbidea:

- 8.2.0 eta geroagoko bertsioen kasuan, segurtasun eguneraketa bertsioan bertan jasota dago.
- 8.1.0.4 eta 8.1.2 bertsioen kasuan, zuzenketa 2019ko iraileko Rollup Patch-en jasota dago, bai eta geroagoko Rollup Patch guztietan ere. Informazio gehiago eskura daiteke Current Isilon OneFS Patches dokumentua irakurriz.
- 8.0.0.7 bertsioaren kasuan, OneFS-ren bertsio berriago batera eguneratzea gomendatzen da.

Xehetasuna:

RAN ez diren HTTP eta WebDAV fitxategien zerbitzuaren osagaiek ahultasun bat daukate. Horietako edozein aktibatuta dagoenean, osagai baterako edo bietarako oinarrizko autentifikazioaz gain, fitxategietarako sarbidea autentifikaziorik gabe egin daiteke. Hori baliatuz urruneko erasotzaile batek murriztutako fitxategietara sarbidea lor lezake. Ahultasun horretarako CVE-2020-5318 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Jenkins-en

Argitalpen data: 2020/01/30

Garrantzia: Altua

Kaltetutako baliabideak:

- Jenkins LTS, 2.204.1 eta lehenagoko bertsioak;
- Jenkins weekly, 2.218 eta lehenagoko bertsioak.

Azalpena:

Jenkins-ek bere *core*-ari eragiten dioten 7 ahultasun antzeman ditu, bat kritikotasun baxukoa, bost ertainekoak eta bat altua. Autentifikaziorik gabeko urruneko erasotzaile batek komunikazioen zifratua arriskuan jar lezake, sisteman zerbitzuaren ukapen egoera eragin edo bertatik informazioa eskuratu.

Konponbidea:

- Jenkins LTS, 2.204.2 bertsiora eguneratzea;
- Jenkins Weekly, 2.219 bertsiora eguneratzea.

Xehetasuna:

- Kritikotasun altuko ahultasunaren jatorria da zifratuaren parametroen berrerabilpen oker bat protokoloan. Autentifikatu gabeko urruneko erasotzaile batek komunikazioen zifratua arriskuan jar lezake, eta kaltetutako Jenkins agenteetatik Jenkins maisura konekta liteke. Ahultasun horretarako CVE-2020-2099 identifikatzailea erabili da.
- Kritikotasun ertaineko ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2020-2100, CVE-2020-2101, CVE-2020-2102, CVE-2020-2103, CVE-2020-2104.
- Kritikotasun baxuko ahultasunari CVE-2020-2105 identifikatzailea esleitu zaio.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Cisco-ren Small Business Switches-en

Argitalpen data: 2020/01/30

Garrantzia: Altua

Kaltetutako baliabideak:

- 2.5.0.92 bertsioa baino lehenagoko firmware-a erabiltzen duten Cisco-ren ondoko produktuak:
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches;
  - 550X Series Stackable Managed Switches.
- 1.4.11.4 bertsioa baino lehenagoko firmware-a erabiltzen duten Cisco-ren ondoko produktuak:
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches.
- 1.3.7.18 bertsioa baino lehenagoko firmware-a erabiltzen duten Cisco-ren ondoko produktuak:
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches.

Azalpena:

DFDR Consulting LLC-ko Ken Pyle ikertzaileak bere Small Business Switches-ek duten kritikotasun altuko bi ahultasunen berri eman dio Cisco-ri. Autentifikaziorik gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake edo gailuetako informazio sentikorrera sarbidea lortu.

Konponbidea:

- Ciscoren ondorengo produktuak firmware-aren 2.5.0.92 bertsiora eguneratzea (CVE-2019-15993):
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches;
  - 550X Series Stackable Managed Switches.
- Ciscoren ondorengo produktuak firmware-aren 1.4.11.4 bertsiora eguneratzea (CVE-2019-15993):
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches.
- Ciscoren ondorengo produktuak firmware-aren 1.3.7.18 bertsiora eguneratzea (CVE-2020-3147):
  - 200 Series Smart Switches;
  - 300 Series Managed Switches;
  - 500 Series Stackable Managed Switches.

Xehetasuna:

- Web erabiltzailearen interfazeak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek asmo gaiztoko HTTP eskaera bat bidal lezake eta gailuaren informazio sentikorra eskuratu. Ahultasun horretarako CVE-2019-15993 identifikatzailea erreserbatu da.
- Web interfazera bidalitako eskaerek duten baliozkotze falta bat baliatuz, urruneko erasotzaile batek asmo gaiztoko eskaerak bidal litzake eta gailuan zerbitzuaren ukapen egoera (DoS) eragin. Ahultasun horretarako CVE-2020-3147 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Zerbitzuaren ukapen erako ahultasuna IBM WebSphere Application Server-en

Argitalpen data: 2020/01/31

Garrantzia: Altua

Kaltetutako baliabideak:

- WebSphere Application Server, honako bertsioak:
  - 9.0;
  - 8.5;
  - 8.0;
  - 7.0.
- WebSphere Application Server Liberty: eguneratze jarraitua.

Azalpena:

Zerbitzuaren ukapen erako larritasun altuko ahultasun bat aurkitu da IBMren WebSphere Application Server-en.

Konponbidea:

- WebSphere Application Server eta WebSphere Application Server Hypervisor Edition-en kasuan, honako bertsioen kasuetan:
  - 0.0.0tik 9.0.5.2ra bitartekoak:
    - *fix pack*-en gutxieneko mailetara eguneratzea *interim fix* PH19528-k (behin-behineko partxea) eskatzen duenaren arabera eta ondoren aplikatzea;
    - 9.0.5.3 *fix pack*-a edo ondorengoa aplikatzea (2020ko lehen hiruhilekorako eskuragarri izatea espero da);
  - 8.5.0.0tik 8.5.5.17ra bitartekoak:
    - fix pack-en paketearen gutxieneko mailetara eguneratzea, PH19528 interim fix-ek eskatzen duenaren arabera, eta ondoren aplikatzea;
    - 8.5.5.18 fix pack-a edo ondorengoa aplikatzea (2020ko hirugarren hiruhilekorako eskuragarri izatea espero da);
  - 8.0.0.0tik 8.0.0.15era bitartean: 8.0.0.15era eguneratzea eta ondoren interim fix PH19528 aplikatzea;
  - 7.0.0.0tik 7.0.0.45era bitartean: 7.0.0.45era eguneratzea eta ondoren interim fix PH19528 aplikatzea.
- WebSphere Application Server Liberty-ren kasuan, transportSecurity-1.0 funtzionaltasuna erabiltzean:
  - fix pack-en gutxieneko mailetara eguneratzea, PH19528 interim fix-ek eskatzen duenaren arabera, eta ondoren aplikatzea;
  - 20.0.0.2 fix pack-a edo ondorengoa aplikatzea (2020ko lehen hiruhilekorako eskuragarri izatea espero da).

Xehetasuna:

IBM WebSphere Application Server ahula da zerbitzuaren ukapen egoera baten aurrean, bereziki diseinatutako eskaera bat bidaliz

eragindakoa. Urruneko erasotzaile batek ahultasun hau balia lezake eskuragarri dagoen memoria guztia zerbitzariak kontsumi dezan eragiteko. Ahultasun horretarako CVE-2019-4720 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Baliozkotze ez-nahikoa OpenBSDren OpenSMTPDren posta zerbitzarian

Argitalpen data: 2020/01/31

Garrantzia: Kritikoa

kaltetutako baliabideak:

OpenSMTPD, honako bertsioak:

- 6.0.2p1-2;
- 6.0.3p1-5;
- 6.6.1p1-5~bpo10 1.

Azalpena:

Qualys Research Labs-eko ikertzaileek ahultasun bat aurkitu dute OpenSMTPDren funtzio batean. Hori baliatuz kode arbitrarioa exekuta liteke *root* baimenekin zerbitzari ahul batean.

Konponbidea:

OpenSMTPD ondoko bertsioetara eguneratzea:

- 6.0.2p1-2 deb9u2;
- 6.0.3p1-5 deb10u3;
- 6.6.2p1-1.

Xehetasuna:

Ahultasuna antzeman da OpenSMTPDek bidaltzailearen helbidea baliozkotzen duen moduan, *smtp_mailaddr*() izena duen funtzio ahularen bidez. Funtzio hori balia daiteke kode arbitrarioa exekutatzeko root baimenekin zerbitzari ahul batean, bereziki diseinatutako SMTP mezu bat bidaliz. Ahultasun horretarako CVE-2020-7247 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Linux, Pribatutasuna, Ahultasuna