2021ko urtarrilaren Bulletina

Ohartarazpenak - Teknikoak

Kredentzial barneratuen motako ahultasuna Zyxel produktuetan

Argitalpen data: 2021/01/05

Garrantzia: Altua

Kaltetutako baliabideak:

Suebakiak:

- ATP series, ZLD 4.60 firmware bertsioa;
- USG series, ZLD 4.60 firmware bertsioa;
- USG FLEX series, ZLD 4.60 firmware bertsioa;
- VPN series, ZLD 4.60 firmware bertsioa;

Sarbide puntuko kontrolatzaileak (AP):

- NXC2500, 6.00tik 6.10erako firmware bertsioak;
- NXC5500, 6.00tik 6.10erako firmware bertsioak;

Azalpena:

EYE Netherlands enpresako Niels Teusink ikertzaileak Zyxel erakundeari eman dio larritasun handiko ahultasun baten berri. Kredentzial barneratuen motakoa da.

Konponbidea:

- Suebakietarako, ZLD V4.60 Patch1 partxea egongo da eskuragarri.
- AP kontroladoreetarako, fabrikatzaileak partxe bat argitaratuko du urtarrilaren 8an.

Xehetasunak:

Kaltetutako produktuek kredentzial barneratuak dituzte, eta, horien bidez, erasotzaile batek administrari pribilegioak lortu litzake, 'zyfwp' erabiltzaile kontuaren bidez. Ahultasun horretarako, CVE-2020-29583 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Hainbat ahultasun Dell EMC Avamar Server sisteman

Argitalpen data: 2021/01/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Dell EMC Avamar Server, 19.1, 19.2, 19.3 bertsioak;
- Dell EMC Integrated Data Protection Appliance (IDPA), 2.5 eta 2.6 bertsioak.

Azalpena:

Dell enpresak jakinarazi du hainbat ahultasun daudela EMC Avamar Server sisteman. Horien bidez, baliteke aplikazio datuetara baimenik gabe sartzea eta irakurtzea, babes-datu konfidentzialak ezabatu edo ateratzea, edota sistema eragilearen komando arbitrarioen exekuzioa gertatzea.

Konponbidea:

Dell etxeak honako hotfix kodeak argitaratu ditu kaltetutako bertsioentzat:

- EMC Avamar Server 19.1: hotfix 325443;
- EMC Avamar Server 19.2: hotfix 325444;
- EMC Avamar Server 19.3: hotfix 325445;
- EMC Integrated Data Protection Appliance (IDPA) 2.5: hotfix: 325443;
- EMC Integrated Data Protection Appliance (IDPA) 2.6: hotfix: 325445;

Xehetasunak:

Dell enpresak jakinarazi du 2 ahultasun kritiko daudela, eta beste bat larritasun handikoa, eta honakoak dira garrantzitsuenak:

- Urrutiko erasotzaile bati, egiaztatu gabe, Fitness Analyzer sisteman, aplikazioaren backend-ean SQL injekzioa burutzeko aukera ematen dion ahultasuna. Ahultasun horretarako, CVE-2020-29493 identifikatzailea esleitu da.
- Sistema eragilearen komandoen injekzio motako ahultasun bat Fitness Analyzer sisteman. Horren bidez, urrutiko erasotzaile batek, egiaztatu gabe, aplikazioaren azpiko sistema eragilearen komando arbitrarioak exekuta litzake. Ahultasun horretarako, CVE-2020-29495 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Pribatutasuna, Ahultasuna

2021eko urtarrileko SAP segurtasunaren eguneratzea

Argitalpen data: 2021/01/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa;
- SAP Business Warehouse, bertsioak: 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755 eta 782;
- SAP BW4HANA, bertsioak: 100 eta 200;
- SAP NetWeaver AS JAVA, bertsioak: 7.10, 7.30, 7.31, 7.40 eta 7.50;
- Automated Note Search Tool (SAP Basis), bertsioak: 7.0, 7.01,7.02, 7.31, 7.4, 7.5, 7.51, 7.52, 7.53 eta 7.54;
- SAP NetWeaver AS Java (HTTP Service), bertsioak: 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50;
- SAP Commerce Cloud, bertsioak: 1808, 1811, 1905, 2005 eta 2011;
- SAP BusinessObjects Business Intelligence platform (Web Intelligence HTML interface), 410 eta 420 bertsioak;
- SAP Master Data Governance, bertsioak: 748, 749, 750, 751, 752, 800, 801, 802, 803 eta 804;
- SAP NetWeaver AS JAVA (Key Storage Service), bertsioak: 7.10, 7.11, 7.20 ,7.30, 7.31, 7.40 eta 7.50;
- SAP GUI FOR WINDOWS, 7.60 bertsioa;
- SAP NetWeaver Master Data Management, bertsioak: 7.10, 7.10.750 eta 710;
- SAP 3D Visual Enterprise Viewer, 9.0 bertsioa;
- SAP Banking Services (Generic Market Data), 400, 450 eta 500 bertsioak;
- SAP EPM ADD-IN, 2.8 eta 1010 bertsioak;

Azalpena:

SAPek produktu batzuen inguruan hainbat segurtasun-eguneratze argitaratu ditu, bere hileroko jakinarazpenean.

Konponbidea:

SAP laguntza-zerbitzua bisitatu eta eguneratze edo partxeak instalatzea, fabrikatzaileak adierazitakoaren arabera.

CVE-2021-21465 ahultasunerako, SAP erakundeak funtzioen modulua desaktibatuz konpondu du arazoa, beraz, modulu horretara deia egiten duen edozein aplikaziori eragingo dio.

Xehetasunak:

SAPek, segurtasun-partxeen hileroko komunikazioan, aurreko oharren 7 eguneratze eta 10 segurtasun ohar egin ditu. Horietako 5 larritasun kritikokoak dira, 1 altukoa, 10 tartekoak eta 1 baxukoa.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Kodearen injekzioaren 2 ahultasun,
- Zerbitzu ukapenaren inguruko ahultasun bat,
- Informazioaren dibulgazioaren arloko 3 ahultasun,
- Baimenaren konprobatze faltaren 4 ahultasun,
- Sarbide-balioztatze ezaren motako 16 ahultasun,
- SQL injekzio arloko ahultasun bat,
- Beste motaren bateko 6 ahultasun.

Segurtasun ohar nabarmenenak honakoen ingurukoak dira:

- SAP Business Warehouse eta SAP BW4HANA sistemen sarbide-balioztatze ez zuzenaren bidez, pribilegio gutxiko erasotzaile batek etengabe txosten gisa gordetzen den kode maltzurra injektatu lezake. Txosten hori gerora exekuta liteke, eta horrek eragin negatibo handia izan lezake sistemaren konfidentzialtasun, integritate eta eskuragarritasunean (eta, agian, konektatutako sistemetan). Ahultasun horretarako, CVE-2021-21466 identifikatzailea

esleitu da.

- SAP BW datu-basearen interfazean SQL komandoen sanitizazio desegokia izatearen ondorioz, erasotzaile batek SQL komando arbitrarioak exekuta litzake datu-basean, beraz, sistema guztiz konprometituta gera liteke. Ahultasun horretarako, CVE-2021-21465 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira:

CVE-2020-26838, CVE-2020-26820, CVE-2021-21446, CVE-2020-6307, CVE-2020-6224, CVE-2021-21445, CVE-2021-21447, CVE-2020-6256, CVE-2020-26816, CVE-2021-21448, CVE-2021-21469, CVE-2021-21449, CVE-2021-21457, CVE-2021-21458, CVE-2021-21459, CVE-2021-21450, CVE-2021-21451, CVE-2021-21452, CVE-2021-21453, CVE-2021-21454, CVE-2021-21455, CVE-2021-21456, CVE-2021-21460, CVE-2021-21461, CVE-2021-21462, CVE-2021-21463, CVE-2021-21464, CVE-2021-21467 eta CVE-2021-21470.

Etiketak: Eguneratzea, SAP, Ahultasuna

Microsoften segurtasun-eguneratzeak. 2021eko urtarrila

Argitalpen data: 2021/01/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows;
- Microsoft Edge (EdgeHTML-based);
- Microsoft Office and Microsoft Office Services and Web Apps;
- Microsoft Windows Codecs Library;
- Visual Studio;
- SQL Server;
- Microsoft Malware Protection Engine;
- .NET Core;
- .NET Repository;
- ASP .NET;
- Azure.

Azalpena:

Segurtasun eguneratzeen inguruko urtarrileko Microsoft argitalpenean 83 ahultasun jaso dira oraingoan; 10 kritiko gisa sailkatu dira eta 73 garrantzitsu gisa.

Konponbidea:

Dagokion segurtasun-eguneratzea instalatzea. Microsoften orrian eguneratze horiek egiteko azalpenak eman dira.

Xehetasunak:

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Kodearen urrutiko exekuzioa.
- Pribilegioak handitzea,
- Zerbitzua ukatzea,
- Informazioa zabaltzea,
- Segurtasun-neurriak saihestea,
- Nortasuna ordeztea (spoofing),
- Manipulazioa (tampering).

Etiketak: Eguneratzea, Microsoft, Nabigatzailea, Ahultasuna, Windows.

Zerbitzu ukapena Junos OS eta Junos OS Evolved sistemetan

Argitalpen data: 2021/01/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Junos OS:

- 17.3R3-S10 bertsioaren aurreko guztiak, salbuespen hauekin: 15.1X49-D240 bertsioa SRX seriean eta 15.1R7-S8 bertsioa EX seriean;
- 17.4, 17.4R2-S12, 17.4R3-S4 bertsioen aurrekoak;
- 18.1, 18.1R3-S12ren aurreko bertsioak;
- 18.2, 18.2R2-S8, 18.2R3-S6 bertsioen aurrekoak;
- 18.3, 18.3R3-S4ren aurreko bertsioak;
- 18.4, 18.4R1-S8 eta 18.4R2-S6, 18.4R3-S6en aurreko bertsioak.

- 19.1, 19.1R1-S6 eta 19.1R2-S2, 19.1R3-S3en aurreko bertsioak.
- 19.2, 19.2R3-S1ren aurreko bertsioak;
- 19.3, 19.3R2-S5, 19.3R3-S1 bertsioen aurrekoak;
- 19.4, 19.4R1-S3 eta 19.4R2-S3, 19.4R3ren aurreko bertsioak.
- 20.1, 20.1R2ren aurreko bertsioak;
- 20.2, 20.2R1-S3 20.2R2ren aurreko bertsioak;
- 20.3 bertsioak, 20.3R1-S1, 20.3R2 aurrekoak.

Junos OS Evolved honako bertsioak:

- 20.3R1-S1-EVO, 20.3R2-EVO bertsioaren aurreko guztiak.

Azalpena:

Juniperrek ahultasun baten berri eman du. Horren bidez, ukapen bat eman liteke Juniper Networks Junos OS eta Junos OS Evolved Routing Protocol Daemon (RPD) zerbitzuetan, BGP FlowSpec mezu espezifiko bat jasotzean.

Konponbidea:

Honako bertsioek ahultasun hori konpontzen dute:

- Junos OS: 15.1R7-S8, 15.1X49-D240, 17.3R3-S10, 17.4R2-S12, 17.4R3-S4, 18.1R3-S12, 18.2R2-S8, 18.2R3-S6, 18.3R3-S4, 18.4R1-S8, 18.4R2-S6, 18.4R3-S6, 19.1R2-S2, 19.1R3-S3, 19.2R3-S1, 19.3R2-S5, 19.3R3-S1, 19.4R1-S3, 19.4R2-S3, 19.4R3, 20.1R2, 20.2R1-S3, 20.2R2, 20.3R1-S1, 20.3R2, 20.4R1, eta osteko guztiak.
- Junos OS Evolved: 20.3R1-S1-EVO, 20.3R2-EVO, 20.4R1-EVO eta osteko guztiak.

Gutxieneko konfigurazio hau behar da arazoa potentzialki konpontzeko: *protocols bgp family inet flow*

Xehetasunak:

Baimen desegokiaren motako ahultasun hori aurkitu da Juniper Networks Junos OS eta Junos OS Evolved Routing Protocol Daemon (RPD) sistemetan, eta, horren bidez, erasotzaile batek BGP FlowSpec mezu baliozko bat bidal lezake, BGP FlowSpec domeinuaren barruko ibilbide-iragarkietan ustekabeko aldaketa sortuz. Mezu horiek bidaltzen jarraituz gero, sareko trafikoan etenak egon daitezke, eta zerbitzuaren ukapena eragin (DoS). Ahultasun horretarako, CVE-2021-0211 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Hainbat ahultasun Jenkins-en

Argitalpen data: 2021/01/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Jenkins Weekly, 2.274 bertsioa eta aurrekoak;
- Jenkins LTS, 2.263.1 bertsioa eta aurrekoak.

Azalpena:

Hainbat ahultasun argitaratu dira Jenkins-en corean, 6 larritasun handikoak, 3 tartekoak eta bat larritasun baxukoa.

Konponbidea:

- Jenkins weekly, 2.275 bertsiora eguneratzea;
- Jenkins LTS, 2.263.2 bertsiora eguneratzea.

Xehetasunak:

Argitaratutako ahultasun motak, larritasun handikoak, honakoekin bat datoz:

- Cross-site Scripting motako (XSS) bi ahultasun. Ahultasun horietarako CVE-2021-21603 eta CVE-2021-21608 identifikatzaileak erreserbatu dira.
- Islatutako Cross-site Scripting motako (XSS) ahultasun bat. Ahultasun horretarako, CVE-2021-21610 identifikatzailea esleitu da.
- Biltegiratutako Cross-site Scripting motako (XSS) ahultasun bat. Ahultasun horretarako, CVE-2021-21611 identifikatzailea esleitu da.
- Fidatzekoak ez diren datuen deserializazio motako ahultasun bat. Ahultasun horretarako, CVE-2021-21604 identifikatzailea esleitu da.
- Sarbide-datuen balioztatze okerraren motako ahultasun 1. Ahultasun horretarako, CVE-2021-21605 identifikatzailea esleitu da.

Gainerako ahultasunetarako, identifikatzaile batzuk esleitu dira: CVE-2021-21602, CVE-2021-21606, CVE-2021-21607 eta CVE-2021-21609.

Etiketak: Eguneratzea, Ahultasuna

XML deserializazio ez segurua Red Hat produktuetan

Argitalpen data: 2021/01/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Decision Manager, 7.9.1 bertsioa;
- Process Automation Manager, 7.9.1 bertsioa.

Azalpena:

Red Hat erakundeak larritasun kritikoko ahultasun bat argitaratu du, XML deserializazio ez seguruaren motakoa.

Konponbidea:

Eguneratzea:

- Process Automation Manager 7.9.1 bertsiora.
- Decision Manager 7.9.1 bertsiora.

Xehetasunak:

Erasotzaile batek urrutiko kodea exekuta lezake, bloke zerrendetako XML deserializazio ez seguru baten ondorioz. Ahultasun horretarako, CVE-2020-26217 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Linux, Ahultasuna

Arubaren AirWave Glass sistemaren ahultasunak

Argitalpen data: 2021/01/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

AirWave Glass, 1.3.2 bertsioa eta aurrekoak.

Azalpena:

Arubak larritasun kritikoko 3 ahultasunen eta larritasun handiko beste baten berri eman du. Horien bidez, web administraziorako interfazean sar liteke baten bat, edo Airwave Glass eremuaren azpiko ostatatze sistema eragilea guztiz konprometitu.

Konponbidea:

1.3.3 edo osteko bertsioen arabera eguneratzea.

Xehetasunak:

- Zerbitzariaren aldean (Server-Side Request Forgery (SSRF)) baimenik gabeko amaierako endpoint baten bidez manipulatutako eskaeren bidez, erasotzaile batek informazio sentikorra zabaldu lezake egiaztatzea saihesteko, eta web administraziorako interfazean administrari sarbidea lortu. Ahultasun horretarako, CVE-2020-24641 identifikatzailea esleitu da.
- Erasotzaile batek komando arbitrarioak exekuta litzake Airwave Glass sistemaren edukiontzi sistema batean, eta azpiko ostatatze sistema eragilea konprometitu. Horretarako, sarbide-datuen balioztatze ez nahikoa edo Javaren deserializazio ez segurua baliatu litzake. Ahultasun horietarako CVE-2020-24640 eta CVE-2020-24639 identifikatzaileak erreserbatu dira.
- Kodearen urrutiko exekuzioaren motako hainbat ahultasun daude Airwave Glass sisteman, cli. Glassadmin bidez, eta, horien bidez, glassadmin pribilegioak dituen erasotzaile batek kode arbitrarioa exekuta lezake, root gisa, azpiko ostatatze zerbitzu eragilean. Ahultasun horretarako CVE-2020-24638 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Dnsmasq-eko ahultasuna

Argitalpen data: 2021/01/21

Garrantzia: Altua

Kaltetutako baliabideak:

Dnsmasq DNS eta DHCP zerbitzaria, 2.8.2 bertsioa eta aurrekoak.

Azalpena:

DNSSEC dnsmasq zerbitzuaren ezarpenean hainbat ahultasun antzeman dira. Horien bidez, urrutiko erasotzaile batek, egiaztatu beharrik gabe, caché-a pozoitu lezake, informazioa zabaldu, kode arbitrarioa exekutatu edota zerbitzuaren ukapena eragin (DoS) kaltetutako gailu batean. Ahultasunak multzokatu eta DNSpooq izena jarri zaie.

Konponbidea:

- Bertsio honetara eguneratzea: dnsmasq 2.83.

- IoT sistema edo sistema barneratuen erabiltzaileek fabrikatzailearekin kontsultatu beharko dute.
- Honako segurtasun praktikak erabiltzea gomendatzen da, DNS azpiegitura babesteko:
    - Babestu DNSko zure bezeroak DNSri segurtasuna ematen dioten stateful-inspection firewalls erabiliz (esaterako, stateful-inspection firewalls delakoak eta NAT gailuek DNSren eskatu gabeko erantzunak blokeatu ditzakete, DNSren aplikazio-geruzaren inspekzioak DNS arraroen paketeak birbidaltzea saihestu lezake).
    - DNSren errekurtsibitate zerbitzu seguru bat ematea, DNSSEC balioztatze eta 0x20 bit kodifikazioarekin, besteak beste, DNSren zerbitzuen barruan, hala dagokionean.
    - IoT gailuak eta bestelako gailuak zuzenean Internet bidez erakusgai ez egotea, DNS abusua minimizatzeko.
    - Inguruarekiko egokia den Secure By Default konfigurazio bat ezartzea.

Xehetasunak:

- DNSSECen datuekin balioztatu aurretik RRSets antolaketa bat egitearen ondorioz, memoria dinamikoan oinarritutako bufferraren gainezkatze motako ahultasun bat (Heap) sortu liteke, eta, horren bidez, erasotzaile batek kode arbitrarioa exekuta lezake bereziki diseinatutako DNS erantzun bat bidaliz. Ahultasun horretarako, CVE-2020-25681 identifikatzailea esleitu da.
- DNSSECen datuekin balioztatu aurretik DNS paketeen izenak ateratzearen ondorioz, memoria dinamikoan oinarritutako bufferraren gainezkatze motako ahultasun bat (Heap) sortu liteke, eta, horren bidez, erasotzaile batek kode arbitrarioa exekuta lezake bereziki diseinatutako DNS erantzun bat bidaliz. Ahultasun horretarako, CVE-2020-25682 identifikatzailea esleitu da.
- Memoria dinamikoan oinarritutako bufferraren gainezkatze motako ahultasunen ondorioz (Heap), DNSSEC aktibatuta dagoenean, jasotako sarbideak balioztatu aurretik, erasotzaile batek zerbitzua ukatu lezake, DNS erantzun baliodunak bidaliz. Ahultasun horietarako CVE-2020-25683 eta CVE-2020-25687 identifikatzaileak esleitu dira.
- Birbidalitako kontsulta baten erantzunean datuen egiazkotasuna behar bezala balioztatzen ez bada Dnsmasq zerbitzua forward.c:reply_query() sisteman konprobatzen ari denean erantzunaren xedeko helbidea / portua egiteke dauden kontsultek erabiltzen duten, erasotzaile batek DNSren caché-a pozoitzeko eraso bat burutu lezake. Ahultasun horretarako, CVE-2020-25684 identifikatzailea esleitu da.
- Algoritmo kriptografiko apurtu edo ahul bat erabiltzearen ondorioz, erasotzaile batek hainbat domeinu ezberdin aurki litzake hash berarekin, ibilbidetik kanpo, Dnsmasq bidez onartzeko erantzun bat faltsutzeko saiakera kopurua nabarmen murriztuz, eta DNSren caché-a pozoitzeko eraso bat burutu. Ahultasun horretarako, CVE-2020-25685 identifikatzailea esleitu da.
- Datuen egiazkotasuna behar den moduan balioztatzen ez bada, kontsulta bat jasotzean Dnsmasq zerbitzuak ez badu konprobatzen izen horrekin beste eskaerarik pendiente dagoen beste eskaera bat birbidali aurretik, erasotzaile batek, sareko ibilbidetik kanpo, Dnsmasq zerbitzuaren bidez onartzeko erantzun bat faltsutzeko saiakera kopurua murriztu lezake, eta DNSren caché-a pozoitzeko eraso bat burutu. Ahultasun horretarako, CVE-2020-25686 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, DNS, Ahultasuna.

Eguneratze kritikoak Oraclen (2011ko urtarrila)

Argitalpen data: 2021/01/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Business Intelligence Enterprise Edition, bertsioak: 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Enterprise Manager Base Platform, bertsioak: 13.2.1.0, 13.3.0.0 eta 13.4.0.0;
- Enterprise Manager for Fusion Applications, 13.3.0.0 bertsioa;
- Enterprise Manager Ops Center, 12.4.0.0 bertsioa;
- Hyperion Financial Reporting, 11.1.2.4 bertsioa;
- Hyperion Infrastructure Technology, 11.1.2.4 bertsioa;
- Instantis EnterpriseTrack, 17.1etik 17.3ra bitarteko bertsioak;
- JD Edwards EnterpriseOne Orchestrator, 9.2.5.1aren aurreko bertsioak;
- JD Edwards EnterpriseOne Tools, 9.2.5.0ren aurreko bertsioak;
- MySQL Client, 5.6.50 bertsioa eta aurrekoak, 5.7.32 bertsioa eta aurrekoak, 8.0.22 eta aurrekoak;
- MySQL Enterprise Monitor, 8.0.22 bertsioa eta aurrekoak;
- MySQL Server, 5.6.50 bertsioa eta aurrekoak, 5.7.32 eta aurrekoak, 8.0.22 eta aurrekoak.
- MySQL Workbench, 8.0.22 bertsioa eta aurrekoak;
- Oracle Adaptive Access Manager, 11.1.2.3.0 bertsioa;
- Oracle Agile Engineering Data Management, 6.2.1.0 bertsioa;
- Oracle Agile PLM, bertsioak: 9.3.5 eta 9.3.6;
- Oracle Agile Product Lifecycle Management for Process, 6.1 bertsioa;
- Oracle Application Express Opportunity Tracker, 20.2aren aurreko bertsio guztiak;
- Oracle Application Express Opportunity Tracker, 20.2aren aurreko bertsio guztiak;
- Oracle Application Testing Suite, 13.3.0.1 bertsioa;
- Oracle Argus Safety, 8.2.2 bertsioa;
- Oracle BAM (Business Activity Monitoring), 11.1.1.9.0 eta 12.2.1.3.0 bertsioa;
- Oracle Banking Corporate Lending Process Management, 14.1.0, 14.3.0 eta 14.4.0 bertsioak;
- Oracle Banking Credit Facilities Process Management, bertsioak: 14.1.0, 14.3.0 eta 14.4.0;
- Oracle Banking Extensibility Workbench, 14.3.0 eta 14.4.0 bertsioak;
- Oracle Banking Liquidity Management, 14.0.0tik 14.4.0ra bitarteko bertsioak;
- Oracle Banking Payments, 14.4.0 bertsioa;
- Oracle Banking Platform, bertsioak: 2.4.0, 2.4.1, 2.6.2, 2.7.0, 2.7.1, 2.8.0 eta 2.9.0;
- Oracle Banking Supply Chain Finance, 14.2.0tik 14.4.0ra bitarteko bertsioak;
- Oracle Banking Trade Finance Process Management, bertsioak: 14.1.0, 14.3.0 eta 14.4.0;
- Oracle Banking Virtual Account Management, bertsioak: 14.1.0, 14.3.0 eta 14.4.0;
- Oracle BI Publisher, bertsioak: 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle Business Intelligence Enterprise Edition, bertsioak: 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle Business Process Management Suite, bertsioak: 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle Coherence, bertsioak: 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 eta 14.1.1.0.0;

- Oracle Communications Application Session Controller, 3.9m0p2 bertsioa;
- Oracle Communications ASAP, 7.3 bertsioa;
- Oracle Communications BRM - Elastic Charging Engine, bertsioak: 11.3.0.9 eta 12.0.0.3;
- Oracle Communications Calendar Server, 8.0.0.4.0 bertsioa;
- Oracle Communications Contacts Server, 8.0.0.5.0 bertsioa;
- Oracle Communications Diameter Signaling Router (DSR), bertsioak: 8.0.0tik 8.2.2ra;
- Oracle Communications Element Manager, bertsioak: 8.2.1.0etik 8.2.2.1era;
- Oracle Communications MetaSolv Solution, 6.3.0tik 6.3.1era bitarteko bertsioak;
- Oracle Communications Network Charging and Control, 6.0.1, 12.0.2 bertsioak;
- Oracle Communications Operations Monitor, bertsioak: 3.4, 4.1, 4.2 eta 4.3;
- Oracle Communications Performance Intelligence Center (PIC) Software, 10.4.0.2 bertsioa;
- Oracle Communications Session Report Manager, 8.2.1.0tik 8.2.2.1era arteko bertsioak;
- Oracle Complex Maintenance, Repair, and Overhaul, bertsioak: 11.5.10, 12.1 eta 12.2;
- Oracle Configurator, 12.1 eta 12.2 bertsioak;
- Oracle Data Integrator, 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak;
- Oracle Database Server, bertsioak: 12.1.0.2, 12.2.0.1, 18c eta 19c;
- Oracle E-Business Suite, bertsioak: 12.1.1etik 12.1.3ra bitartekoak, eta 12.2.3tik 12.2.10era bitartekoak;
- Oracle Endeca Information Discovery Integrator, 3.2.0.0 bertsioa;
- Oracle Enterprise Communications Broker, 3.1 eta 3.2 bertsioak;
- Oracle Enterprise Data Quality, 11.1.1.9.0 eta 12.2.1.3.0 bertsioak;
- Oracle Enterprise Repository, 11.1.1.7.0 bertsioa;
- Oracle Financial Services Analytical Applications Infrastructure, 8.0.6tik 8.1.0era bitarteko bertsioak;
- Oracle Financial Services Asset Liability Management, 8.0.7 eta 8.1.0 bertsioak;
- Oracle Financial Services Data Integration Hub, 8.0.3 eta 8.0.6 bertsioak;
- Oracle Financial Services Funds Transfer Pricing, bertsioak: 8.0.6, 8.0.7, 8.1.0;
- Oracle Financial Services Market Risk Measurement and Management, 8.0.6 bertsioa;
- Oracle Financial Services Profitability Management, 8.0.6, 8.0.7, 8.1.0 bertsioak;
- Oracle Financial Services Revenue Management and Billing, 2.9.0.0 eta 2.9.0.1 bertsioak;
- Oracle FLEXCUBE Core Banking, 11.5.0tik 11.9.0ra bitarteko bertsioak;
- Oracle FLEXCUBE Universal Banking, 14.4.0 bertsioa;
- Oracle Fusion Middleware MapViewer, 12.2.1.3.0 bertsioa;
- Oracle Global Lifecycle Management OPatch;
- Oracle Global Lifecycle Manager;
- Oracle GoldenGate Application Adapters, 19.1.0.0.0 bertsioa;
- Oracle GraalVM Enterprise Edition, 19.3.4 eta 20.3.0 bertsioak;
- Oracle Health Sciences Information Manager, 3.0.1 bertsioa;
- Oracle Healthcare Master Person Index, 4.0.2.5 bertsioa;Oracle Hospitality Reporting and Analytics, 9.1.0 bertsioa;
- Oracle Hospitality Simphony, bertsioak: 18.2.7.2 eta 19.1.3;
- Oracle Insurance Allocation Manager for Enterprise Profitability, 8.1.0 bertsioa;
- Oracle Insurance Insbridge Rating and Underwriting, 5.0.0.20 eta 5.1.1.3 bertsioak;
- Oracle Insurance Policy Administration, bertsioak: 10.2.0, 10.2.4, 11.0.2 eta 11.1.0tik 11.3.0ra bitartekoak;
- Oracle Insurance Rules Palette, bertsioak: 10.2.0, 10.2.4, 11.0.2 eta 11.1.0tik 11.3.0ra bitartekoak;
- Oracle Java SE, 7u281 eta 8u271 bertsioak;
- Oracle Java SE Embedded, 8u271 bertsioa;
- Oracle Managed File Transfer, bertsioak: 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle Outside In Technology, 8.5.4 eta 8.5.5 bertsioak;
- Oracle Real-Time Decision Server, 3.2.1.0 bertsioa;Oracle Retail Assortment Planning, 16.0.3 bertsioa;
- Oracle Retail Bulk Data Integration, 15.0.3 eta 16.0.3 bertsioak;
- Oracle Retail Customer Management and Segmentation Foundation, 16.0, 17.0, 18.0 eta 19.0 bertsioak;
- Oracle Retail Extract Transform and Load, 13.2.5 eta 13.2.8 bertsioak;
- Oracle Retail Financial Integration, 14.1.3, 15.0.3 eta 16.0.3 bertsioak;
- Oracle Retail Integration Bus, 14.1.3, 15.0.3 eta 16.0.3 bertsioak;
- Oracle Retail Invoice Matching, 13.2, 14.0 eta 14.1 bertsioak;
- Oracle Retail Merchandising System, 15.0 bertsioa;
- Oracle Retail Order Broker, 15.0 eta 16.0 bertsioak;
- Oracle Retail Order Broker Cloud Service, 15.0 bertsioa;
- Oracle Retail Sales Audit, 14.1 bertsioa;
- Oracle Retail Service Backbone, 14.1.3, 15.0.3 eta 16.0.3 bertsioak;
- Oracle Retail Store Inventory Management, bertsioak: 14.0.4.0, 14.1.3.0, 14.1.3.9, 15.0.3.0 eta 16.0.3.0;
- Oracle SD-WAN Edge, 9.0 bertsioa;
- Oracle Secure Backup;
- Oracle Transportation Management, 1.4.3 bertsioa;
- Oracle Utilities Framework, bertsioak: 4.2.0.2.0, 4.2.0.3.0, de la 4.3.0.1.0 a la 4.3.0.6.0, 4.4.0.0.0 eta 4.4.0.2.0;
- Oracle VM VirtualBox, 6.1.18 bertsioaren aurreko guztiak;
- Oracle WebCenter Portal, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle WebCenter Sites, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak;
- Oracle WebLogic Server, bertsioak: 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 eta 14.1.1.0.0;
- Oracle ZFS Storage Appliance Kit, 8.8 bertsioa;
- PeopleSoft Enterprise FIN Payables, 9.2 bertsioa;
- PeopleSoft Enterprise HCM Human Resources, 9.2 bertsioa;
- PeopleSoft Enterprise PeopleTools, 8.56, 8.57 eta 8.58 bertsioak;
- Primavera Gateway, bertsioak: 16.2.0tik 16.2.11ra, 17.12.0tik 17.12.9ra, 18.8.0tik 18.8.10era eta 19.12.0tik a la 19.12.10era bitartekoak;
- Primavera P6 Enterprise Project Portfolio Management, bertsioak: 16.1.0tik 16.2.20ra, 17.1.0ra 17.12.19ra, 18.1.0tik 18.8.21era eta 19.12.0tik a la 19.12.10era bitartekoak;
- Primavera Unifier, bertsioak: 16.1, 16.2, 17.7tik 17.12ra bitartekoak, 18.8, 19.12 eta 20.12;
- Siebel Applications, 20.12 bertsioa eta aurrekoak;
- StorageTek Tape Analytics SW Tool, 2.3.1 bertsioa;

Azalpena:

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

Konponbidea:

Kaltetutako produktuen araberako partxeak aplikatzea. Eguneratzeak deskargatzeko informazioa Oraclek argitaratutako segurtasun buletinean eskura daiteke.

Xehetasunak:

Eguneratze horrek 329 ahultasun konpontzen ditu, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna Oracleren loturan dagoen Erreferentzien atalean kontsulta daiteke.

Etiketak: Eguneratzea, Oracle, Ahultasuna

Ahultasuna Drupal etxearen core-an

Argitalpen data: 2021/01/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Hauen aurreko bertsioak:

- 9.1.3;
- 9.0.11;
- 8.9.13;
- 7.78.

Azalpena:

Larritasun kritikoko ahultasun bat argitaratu da, Archive_Tar liburutegian, eta Drupalen core-ari eragiten dio.

Konponbidea:

Bertsio hauetara eguneratzea: 9.1.3, 9.0.11, 8.9.13 edo 7.78.

Drupal 8-ren 8.9.x bertsioaren aurrekoak azkenetan daude eta ez dute segurtasun estaldurarik jasotzen.

Xehetasunak:

Archive_Tar liburutegiko lotura sinbolikoak behar ez bezala konprobatzearen ondorioz, eskritura operazioak egin litezke Directory Traversal tresnarekin. Ahultasun horretarako, CVE-2020-36193 identifikatzailea esleitu da.

Etiketak: Eguneratzea, CMS, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2021/01/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco DNA Center Software, 1.3.1.0 bertsioa eta aurrekoak;
- Cisco Smart Software Manager Satellite, 5.1.0 bertsioa eta aurrekoak;
- Honako produktuak, Cisco SD-WAN Solution Software sistemaren bertsio ahul bat exekutatzen ari badira:
  - SD-WAN vBond Orchestrator Software;
  - SD-WAN vEdge Cloud Routers;
  - SD-WAN vEdge Routers;
  - SD-WAN vManage Software;
  - SD-WAN vSmart Controller Software;
  - IOS XE SD-WAN Software.

Azalpena:

14 ahultasun antzeman dira Cisco produktuetan. Horietatik 6 ahultasun kritikokoak dira, eta, horien bidez, urrutiko erasotzaile batek komando arbitrarioak exekuta ditzake, edo bufferraren gainezkatzea eragin.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneratzeak Ciscoren Software deskarga panelean deskargatu daitezke. Informazio zehatzagoa izateko, kontsultatu Erreferentzien atala.

Xehetasunak:

Urrutiko erasotzaile batek, egiaztatu gabe, komando arbitrarioak exekuta litzake SD-WAN vManage Software-ren web erabiltzaile interfazean, DNA Center-eko Command Runner tresnan edo Smart Software Manager Satellite webgunearen interfazean sartzea lortuz gero, bereziki diseinatutako sarbide bat bidalita. Ahultasun horietarako CVE-2021-1299, CVE-2021-1264, CVE-2021-1138, CVE-2021-1140 eta CVE-2021-1142 identifikatzaileak esleitu dira.

IP trafikoaren erabilera desegokiaren ahultasun baten ondorioz, erasotzaile batek bereziki diseinatutako IP trafikoa bidal lezake, eta bufferraren gainezkatzea eragin. Ahultasun horretarako, CVE-2021-1300 identifikatzailea esleitu da.

Larritasun handiko ahultasunei honakoak esleitu zaizkie: CVE-2021-1261, CVE-2021-1260, CVE-2021-1139 eta CVE-2021-1141.

Tarteko larritasuneko ahultasunei honakoak esleitu zaizkie: CVE-2021-1263, CVE-2021-1262, CVE-2021-1298 eta CVE-2021-

1301.

Etiketak: Eguneratzea, Cisco, Ahultasuna

Hainbat ahultasun Moodle-n

Argitalpen data: 2021/01/25

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- 3.10 bertsioa;
- 3.9 bertsiotik 3.9.3 bertsiora bitartekoak;
- 3.8 bertsiotik 3.8.6 bertsiora bitartekoak;
- 3.5 bertsiotik 3.5.15 bertsiora bitartekoak;
- zerbitzurik gabeko lehenagoko bertsioak.

Azalpena:

Moodle-k dituen 5 ahultasunen berri eman da, 3 larritasun kritikokoak eta 2 larritasun baxukoak. Horiek baliatuz XSS erako erasoak egin litezke, PHP kode arbitrarioa exekutatu, informazioa hedatu edo bezeroaren aldean zerbitzuaren ukapena eragin.

Konponbidea:

Ondoko eguneraketak aplikatzea, kaltetutako bertsioaren arabera:

- 3.10.1;
- 3.9.4;
- 3.8.7;
- 3.5.16.

Xehetasunak:

- Sarreren bilaketaren txantiloitik bilaketa kontsulten baliozkotze ez-nahikoa baliatuz, erasotzaile batek islatutako XSS erasoak egin litzake. Ahultasun horretarako CVE-2021-20183 identifikatzailea erabili da.
- TeX notazio iragazkia aktibatuta dagoenean TeX edukiaren saneatze ez-aski bat baliatuz, erasotzaile batek biltegiratutako XSS erako erasoak egin litzake. Ahultasun horretarako CVE-2021-20186 identifikatzailea erabili da.
- Gunearen administratzaileek PHP script arbitrarioak exekuta litzakete PHP include baten bidez, Shibboleth-en autentifikazioa egiten den bitartean erabilitakoa. Ahultasun horretarako CVE-2021-20187 identifikatzailea erabili da.

Larritasun baxuko gaineko ahultasunetarako CVE-2021-20184 eta CVE-2021-20185 identifikatzaileak erabili dira.

Etiketak: Eguneraketa, CMS, Ahultasuna

0-day erako ahultasuna SonicWall-en SMA 100-en

Argitalpen data: 2021/01/25

Garrantzia: Altua

Kaltetutako baliabideak:

Ikertuak izaten ari diren produktuak SMA 100 Series-ekoak dira (SMA 200, SMA 210, SMA 400, SMA 410 eta SMA 500v Virtual appliance).

Azalpena:

SonicWall-ek jarraitzen du ikertzen 0-day erako balizko ahultasun bat, larritasun altukoa.

Konponbidea:

Ikerkuntzak irauten duen bitartean SMA 100 serieko administratzaileei honakoa eskatzen zaie:

- Firewall bat erabiltzea, SMA aplikaziora SSL-VPN konexioak IP ezagunetatik edo zerrenda zuri batean jasotakoetatik soilik baimentzen dituzten arauak dituena. Horretarako honako esteka kontsultatu.
- Sarbide arau bereziak sortzea edo Internetetik HTTPS eta Virtual Offfice bidezko sarbide administratiboa desgaitzea, ikerkuntzak irauten duen bitartean.

Xehetasunak:

SonicWall-ek bere barne sistemen aurkako eraso koordinatu bat identifikatu zuen oso sofistikatuak ziren mehatxuen egileen aldetik. Horiek 0-day erako balizko ahultasunak baliatzen zituzten SonicWall-en urruneko sarbide seguruko produktu jakin batzuetan.

Etiketak: 0day, Komunikazioak, Ahultasuna

Zerbitzuaren ukapen erako ahultasuna Xen-en

Argitalpen data: 2021/01/27

Garrantzia: Altua

Kaltetutako baliabideak:

Xen, 4.12.3 eta 4.12.4 bertsioak eta 4.13.1 bertsioak eta ondorengo guztiak.

Azalpena:

Xen-ek jakinarazi du x86 sistemetan ahultasun bat dagoela. Horren bitartez PCI pass through gailuak dituen HVM gonbidatu batek beste gonbidatu batzuen edo host osoaren PCI baliabide eskuragarriak agor ditzake, zerbitzuaren ukapena eraginez.

Konponbidea:

Xen-ek partxe bat argitaratu du 4.14 - 4.12 bertsioetarako eta unstable bertsiorako.

Xehetasunak:

Aurkitutako ahultasunak soilik eragiten die PCI pass through gailuekin HVM gonbidatuak exekutatzen dituzten x86 sistemei. Erasotzaile batek sistemako IDT bektore guztien esleipena bortxa lezake, PCI baliabideak agortzea eraginez eta horrela zerbitzuaren ukapena sortuz. Ahultasun horretarako CVE-2021-3308 identifikatzailea erabili da.

Etiketak: Eguneraketa, Birtualizazioa, Ahultasuna

Bufferraren gainezkatze erako ahultasuna sudo-n

Argitalpen data: 2021/01/27

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Sudo, honako bertsioak:

- 1.8.2 bertsiotik 1.8.31p2 bertsiora bitartekoak;
- 1.9.0 bertsiotik 1.9.5p1 bertsiora bitartekoak.

Azalpena:

Qualys Research Team-ek ahultasun baten berri eman dio sudo-ri, memoria dinamikoan (heap) oinarritutako bufferraren gainezkatze erakoa, pribilegioak eskalatzea ahalbidetu lezakeena.

Konponbidea:

sudo-ren 1.9.5p2 bertsiora eguneratzea.

Xehetasunak:

Ahultasuna, bere aurkitzaileek Baron Samedit izendatu dutena, autentifikatu gabeko edozein erabiltzaile lokalek balia lezake root mailako pribilegioetaraino eskalatzeko, baita erabiltzailea sudoers fitxategian ageri ez bada ere. Akatsa dago komandoen argumentuetan karaktere bereziak ihes egiten dituen kodean, sudo-k shell moduan komando bat exekutatzen duenean. Ahultasun horretarako CVE-2021-3156 identifikatzailea erabili da.

Etiketak: Eguneraketa, Linux, Ahultasuna

0day erako hainbat ahultasun Apple-n produktuetan

Argitalpen data: 2021/01/27

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- iOS, 14.4 baino lehenagoko bertsioak;
- iPadOS, 14.4 baino lehenagoko bertsioak.

Azalpena:

Ikertzaile anonimo batek 0day erako hiru ahultasunen berri eman dio Apple-ri. Horiek baliatuz erasotzaile batek pribilegioen eskalatzea egin lezake edo kode arbitrarioa exekutatu urrunetik.

Konponbidea:

iOS 14.4 eta iPadOS 14.4 bertsioetara eguneratzea, web-ean adierazitako pausoak jarraituz. Ondoko produktuetarako daude eskuragarri:

- iPhone 6s eta ondorengoak,
- iPad Air 2 eta ondorengoak, iPad mini 4 eta ondorengoak,
- iPod touch (zazpigarren belaunaldia).

Xehetasunak:

- Asmo gaiztoko aplikazio batek erasotzaile bati ahalbidetu liezaioke pribilegioen eskalatzea egitea, Kernel-ari eragiten dion lasterketaren egoera erako ahultasun bat baliatuz. Ahultasun horretarako CVE-2021-1782 identifikatzailea erabili da.
- Urruneko erasotzaile batek kode arbitrarioa exekuta lezake WebKit-ari eragiten dioten logika ahultasunak baliatuz. Ahultasun horietarako CVE-2021-1871 eta CVE-2021-1870 identifikatzaileak erabili dira.

Applek jakinarazi du ahultasun hauek agian aktiboki baliatuak izan direla.

Etiquetas: 0day, Eguneraketa, Apple, Ahultasuna