2021ko Apirilaren Bulletina

Ohartarazpenak - Teknikoak

URL kudeaketa okerraren motako ahultasuna VMware Carbon Black Cloud Workload eremuan

Argitalpen data: 2021/04/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

VMware Carbon Black Cloud Workload, 1.0.1 bertsioa eta aurrekoak, Linux sisteman exekutatzen.

Azalpena:

Egor Dimitrenkok, Positive Technologies erakundeko ikertzaileak, larritasun kritikoko ahultasun baten berri eman dio VMware erakundeari. Horren bidez, erasotzaile batek pribilegioetan gora egin lezake, URL kudeaketa oker baten ondorioz.

Konponbidea:

VMware Carbon Black Cloud Workload 1.0.2 bertsiora eguneratzea.

Xehetasuna:

Erasotzaile batek, VMware Carbon Black Cloud Workload gailuaren interfaze administratiborako sare-sarbidearekin, egiaztatze token baliagarri bat lortu lezake, gailuaren administrazio APIrako sarbidea emanez. Ahultasun hori arrakastaz baliatuta, erasotzaileak konfigurazio administratiboaren doikuntzak ikusi eta aldatu litzake. Ahultasun horretarako, CVE-2021-21982 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Birtualizazioa, VMware, Ahultasuna.

Hainbat ahultasun Cisco produktu batzuetan

Argitalpen data: 2021/04/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco Small Business routerrak:
  - RV110W Wireless-N VPN Firewall;
  - RV130 VPN Router;
  - RV130W Wireless-N Multifunction VPN Router;
  - RV215W Wireless-N VPN Router.
- Software SD-WAN vManage, 18.4 bertsioa eta aurrekoak, 19.2, 19.3, 20.1, 20.3 eta 20.4

Azalpena:

Larritasun kritikoko 2 ahultasun eta larritasun handiko beste 2 ahultasun antzeman dira. Horien bidez, erasotzaile batek, urrunetik eta baimenik gabe, pribilegioetan gora egin lezake, edo kode arbitrarioa exekutatu.

Konponbidea:

SD-WAN vManage softwarearen kasuan, 19.2.4, 20.3.3 eta 20.4.1 bertsio egonkorretara eguneratzea gomendatzen da, hurrenez hurren.

Routerren kasuan, RV132W, RV160 edo RV160W produktuetara migratzea gomendatzen da, izan ere, ez da eguneratzerik argitaratuko bizitza erabilgarriaren amaierara helduta.

Xehetasuna:

Ahultasun kritikoak honakoei dagozkie:

- SD-WAN vManage softwarearen urruneko kudeatzaileak sarrera-datuak modu desegokian balioztatzearen ondorioz, erasotzaile batek, urrunetik eta baimenik gabe, bufferraren gainezkatzea eragin lezake eta kode arbitrarioa exekutatu azpiko sistema eragilean, root pribilegioekin, bereziki diseinatutako konexio-eskaera bat bidali ostean. Ahultasun kritiko horretarako, CVE-2021-1479 identifikatzailea esleitu da.
- Kaltetutako routerren webgunean oinarritutako administrazio-interfazean datuak oker balioztatzearen ondorioz, erasotzaile batek, urrunetik eta baimenik gabe, kode arbitrarioa exekuta lezake root erabiltzaile gisa azpiko sistema eragilean, bereziki diseinatutako HTTP eskaerak bidaliz. Ahultasun kritiko horretarako, CVE-2021-1459 identifikatzailea esleitu da.

Kritikotasun handiko gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2021-1137 eta CVE-2021-1480.

Etiketak: Eguneratzea, Cisco, Komunikazioak, Ahultasuna.

Hainbat ahultasun Synology produktu batzuetan

Argitalpen data: 2021/04/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- DiskStation Manager (DSM), 6.2 bertsioa;
- DSM UC, 3.0 bertsioa;
- SkyNAS;
- VS960HD.

Azalpena:

Larritasun kritikoko 6 ahultasun eta larritasun handiko beste 6 ahultasun antzeman dira. Horien bidez, erasotzaile batek kode arbitrarioa exekutatu lezake.

Konponbidea:

DSM produktuaren kasuan, 6.2.3-25426-3 bertsiora edo osteko batera eguneratzea.

Gainerako produktuetarako ez dago konponbiderik, momentuz.

Xehetasunak:

- Karrera baldintzako ahultasun baten, Use-After-Free motako ahultasun baten edota mugetatik kanpoko irakurketaren motako ahultasun baten (DSMren iscsi_snapshot_comm_core sisteman) bidez, urruneko erasotzaile batek kode arbitrarioa exekuta lezake bereziki diseinatutako web konponbideen bidez. Ahultasun kritiko horietarako CVE-2021-26569, CVE-2021-27646 eta CVE-2021-27647 identifikatzaileak esleitu dira.
- Informazio konfidentziala duen zifratu gabeko testu baten transmisio motako ahultasunaren, pilan oinarritutako bufferraren gainezkatze motako ahultasun baten, edota mugetatik kanpoko idazketaren motako ahultasun baten bidez (DSMren synoagentregisterd sisteman), man-in-the-middle erasoak burutu litezke zerbitzariak faltsutu edota kode arbitrarioa exekutatzeko, hurrenez hurren. Ahultasun kritiko horietarako CVE-2021-26560, CVE-2021-26561 eta CVE-2021-26562 identifikatzaileak esleitu dira.

Gainerako ahultasunetarako, identifikatzaile hauek esleitu dira: CVE-2021-26563, CVE-2021-26564, CVE-2021-26565, CVE-2021-26566, CVE-2021-26567 eta CVE-2021-29083.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Microsoften segurtasun-eguneratzeak. 2021eko apirila.

Argitalpen data: 2021/04/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Azure AD Web Sign-in,
- Azure DevOps,
- Azure Sphere,
- Microsoft Edge (basado en Chromium),
- Microsoft Exchange Server,
- Microsoft Graphics Component,
- Microsoft Internet Messaging API,
- Microsoft NTFS,
- Microsoft Office Excel,

- Microsoft Office Outlook,
- Microsoft Office SharePoint,
- Microsoft Office Word,
- Microsoft Windows Codecs Library,
- Microsoft Windows Speech,
- Open Source Software,
- Role: DNS Server,
- Role: Hyper-V,
- Visual Studio,
- Visual Studio Code,
- Visual Studio Code - GitHub Pull Requests e Issues Extension,
- Visual Studio Code - Kubernetes Tools,
- Visual Studio Code - Maven para Java Extension,
- Windows Application Compatibility Cache,
- Windows AppX Deployment Extensions,
- Windows Console Driver,
- Windows Diagnostic Hub,
- Windows Early Launch Antimalware Driver,
- Windows ELAM,
- Windows Event Tracing,
- Windows Installer,
- Windows Kernel,
- Windows Media Player,
- Windows Network File System,
- Windows Overlay Filter,
- Windows Portmapping,
- Windows Registry,
- Windows Remote Procedure Call Runtime,
- Windows Resource Manager,
- Windows Secure Kernel Mode,
- Windows Services and Controller App,
- Windows SMB Server,
- Windows TCP/IP,
- Windows Win32K,
- Windows WLAN Auto Config Service.

Azalpena:

Segurtasun eguneratzeen inguruko Microsoft argitalpenean 117 ahultasun jaso dira; 19 kritiko gisa sailkatu dira, 89 garrantzitsu gisa, eta 9 oraindik larritasun-mailarik esleitu gabe.

Konponbidea:

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

Xehetasunak:

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Zerbitzua ukatzea.
- Pribilegioak handitzea.
- Informazioa zabaltzea.
- Kodearen urrutiko exekuzioa.
- Segurtasun funtzioaren omisioa.
- Nortasuna ordeztea (spoofing).

Microsoftek 5 0day ahultasun zuzendu ditu, honako identifikatzaileekin: CVE-2021-27091, CVE-2021-28312, CVE-2021-28437, CVE-2021-28458 eta CVE-2021-28310 (azken hau aktiboki baliatzen ari dira).

GARRANTZITSUA: NSA erakundeak kodearen urruneko exekuzioaren motako 4 ahultasun kritikoren berri eman du; Microsoft Exchange Server (2013, 2016 eta 2019) sistemari eragiten diote, eta buletin honetan konpondu dira (2013 CU23; 2016 CU19 y CU20, eta 2019 CU8 y CU9). Identifikatzaileak honakoak dira: CVE-2021-28480, CVE-2021-28481, CVE-2021-28482 eta CVE-2021-28483.

Etiketak: 0day, Eguneratzea, Komunikazioak, DNS, Azpiegitura kritikoak, Nabigatzailea, Pribatutasuna, Birtualizazioa, Ahultasuna, Windows.

NAME: WRECK, hainbat ahultasun DNS sisteman

Argitalpen data: 2021/04/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

DNS inplementazioak TCP/IP piletan: FreeBSD, Nucleus NET, IPnet eta NetX.

Azalpena:

Forescout Research Labs erakundeak, JSOF Research erakundearekin elkarlanean, NAME:WRECK errebelatu du, lau TCP/IP pila ospetsuri eragiten dien bederatzi ahultasuneko multzoa (FreeBSD, Nucleus NET, IPnet eta NetX). Ahultasun horiek zerikusia dute Domeinu Izenen Sistemaren inplementazioekin (DNS), eta zerbitzuaren ukapena (DoS) edota kodearen urruneko exekuzioa (RCE) eragin dezakete. Horrela izanik, erasotzaileek gailuak deskonektatu edota horien kontrola hartu ahal izango lukete.

Konponbidea:

- NAME:WRECK multzoaren aurkako babes osoa izateko, IP pilen bertsio ahulak exekutatzen dituzten gailuak partxeatu behar dira. FreeBSD, Nucleus NET eta NetX duela gutxi partxeatu dira, eta software hori erabiltzen duten gailuen hornitzaileek beren eguneratzeak eskaini beharko lizkiekete bezeroei. Baliteke eguneratze horiek denboran luzatzea eta berehala ez argitaratzea, konplexutasuna eta kasuistika bereziak direla eta. DNS edo DHCP konponketarako zerbitzuak gehitzen dituen edozein produktu erabiltzen dutenei gomendatzen zaie denboran zehar fabrikatzaileak egiten dituen eguneratzeak errebisatzeko, ahultasun horiek konpontze aldera.

Hala ere, beti ez da posible gailuak partxeatzea, eta egin beharreko ahalegina guztiz aldatzen da gailua TI zerbitzari estandar bat edo IoT gailu bat izanda. Erronka horiek kontuan izanda, honako arintze-estrategia gomendatzen da:

- Pila ahulak exekutatzen dituzten gailuen inbentarioa egitea. Forescout Research Labs erakundeak script ireki bat argitaratu du. Aztarna digitala erabiltzen du kaltetutako pilak exekutatzen dituzten gailuak antzemateko. Scripta etengabe erabiltzen da sinadura berriekin, ikerketaren azken garapena jarraitzeko. eyeSight erabiltzen duten Forescout bezeroek FreeBSD, Nucleus RTOS, ThreadX edo VxWorks erabiltzen duten gailuak automatikoki identifika ditzakete.
- Segmentazio kontrolak eta sareko bastionatze egokiak aplikatzea gailu ahulen arriskua arintzeko. Mugatu kanpo komunikazioak eta isolatu edo eutsi gailu ahulei arintze kontrolerako eremuetan, ezin badira partxeatu, edota partxeatu ahal izan arte.
- Kaltetutako gailuen hornitzaileek argitaratutako partxe progresiboak gainbegiratzea eta aktibo ahulen inbentariorako berreskuratze-plan bat diseinatzea, enpresa-arriskua eta negozioaren iraupenerako baldintzak orekatuz.
- Gailuak konfiguratzea, posible den neurrian barneko DNS zerbitzarien mende egoteko, eta kanpo DNS trafikoa zehazki gainbegiratzea, izan ere, esplotazioak eskatzen du DNS zerbitzari maltzur batek pakete maltzurrekin erantzutea.
- Sareko trafiko guztia gainbegiratzea, DNS, mDNS eta DHCP bezeroei eragiten dieten 0-day posibleak edota ahultasun ezagunak baliatzeko asmoa duten pakete maltzurren bila. Trafiko ezohikoa edo gaizki eratutakoa blokeatu egin beharko litzateke, edo, behintzat, sareko eragileei horren berri eman. NAME:WRECK multzoko ahultasunak baliatzeko, erasotzaileak edozein TCP/IP pilarako antzeko prozedura erabili beharko luke. Horrek esan nahi du NAME:WRECK multzoaren erabilera identifikatzeko erabilitako teknika baliagarria izango litzatekeela beste TCP/IP pila batzuetan, eta oraindik aztertu ez diren produktuetan erabilera antzemateko. Gainera, AMNESIA:33ren parte gisa entregatutako mehatxuak antzemateko SD scripta aktibatu zuten Forescout eyeInspect-en bezeroek NAME:WRECK multzoaren erabilera antzeman dezakete.

Xehetasunak:

- DHCP paketeetan dhclient(8) 119 aukeraren datuak aztertzerakoan muga-akats bat gertatzearen ondorioz, urruneko erasotzaile batek, tokiko sarean, bereziki diseinatutako datuak bidali ahalko lizkioke DHCP bezeroari, pilan oinarritutako bufferraren gainezkatzea eragin, eta xedeko sisteman kode arbitrarioa exekutatu. Ahultasun horretarako, CVE-2020-7461 identifikatzailea esleitu da.
- DNS bezeroaren mezuen deskonpresio-funtzioan pilan oinarritutako bufferraren gainezkatzearen ondorioz, erasotzaile batek kodearen urruneko exekuzioa bideratu lezake (RCE). Ahultasun horretarako CVE-2016-20009 identifikatzailea esleitu da, hau da, larritasun handienekoa, 9.8ko CVSSarekin.
- DNS domeinuko izenen etiketen azterketaren funtzionalitateak ez ditu behar den moduan balioztatzen DNS erantzunen izenak. Gaizki eratutako erantzunen analisi sintaktikoaren bidez, esleitutako egitura baten amaieratik haragoko idazketa bat eragin lezake. Erasotzaile batek, sareko posizio pribilegiatu batetik, ahultasun hori baliatu lezake egungo prozesuaren testuinguruan kodea exekutatzeko edota zerbitzuaren ukapena eragiteko. Ahultasun horretarako, CVE-2020-15795 identifikatzailea esleitu da.
- DNS domeinuaren izenen erregistroaren deskonpresioaren funtzionalitateak ez ditu behar den moduan balioztatzen punteroaren leku-aldatze balioak. Erasotzaile batek DNS erantzuna emateko pakete bat egin lezake, bereziki diseinatua, eta, horren bidez, datu arbitrarioak idatzi ahal izango lituzke gailu baten memoriaren parte sentikorretan, eta, ostean, kodea injektatuko luke. Ahultasun horretarako, CVE-2020-27009 identifikatzailea esleitu da.
- DNS domeinuko izenen etiketen azterketaren funtzionalitateak ez ditu behar den moduan balioztatzen DNS erantzunen izenak. Gaizki eratutako erantzunen analisiaren ondorioz, irakurketa bat egin liteke esleitutako egitura baten amaieratik harago. Erasotzaile batek, sareko posizio pribilegiatu batetik, ahultasun hori baliatu lezake zerbitzuaren ukapena eragiteko. Ahultasun horretarako, CVE-2020-27736 identifikatzailea esleitu da.
- DNS erantzunaren analisiaren funtzionalitateak ez ditu behar bezala balioztatzen erregistroen kontaketak eta hainbat luzera. Gaizki eratutako erantzunen analisi sintaktikoaren ondorioz, irakurketa bat egin liteke esleitutako egitura baten amaieratik harago. Erasotzaile batek, sareko posizio pribilegiatu batetik, ahultasun hori baliatu lezake zerbitzuaren ukapena eragiteko. Ahultasun horretarako, CVE-2020-27737 identifikatzailea esleitu da.
- DNS domeinuaren izenen erregistroaren deskonpresioaren funtzionalitateak ez ditu behar den moduan balioztatzen punteroaren leku-aldatze balioak. Gaizki eratutako erantzunen analisi sintaktikoaren ondorioz, irakurketa bat egin liteke esleitutako egitura baten amaieratik harago. Erasotzaile batek, sareko posizio pribilegiatu batetik, ahultasun hori baliatu lezake zerbitzuaren ukapena eragiteko. Ahultasun horretarako, CVE-2020-27738 identifikatzailea esleitu da.
- DNS bezeroak ez ditu behar den moduan ausazko bihurtzen DNS (TXID) transakzioaren ID eta UDP portuko zenbakiak, beraz, erasotzaile batek DNS cachea pozoitzearen eta nortasuna ordeztearen motako erasoak burutu litzake. Ahultasun horretarako, CVE-2021-25677 identifikatzailea esleitu da.
- DNS osagaian, _nx_dns_name_string_unencode eta _nx_dns_resource_name_real_size_calculated funtzioek ez dute konprobatzen konpresio-punteroa ez denik egun aztertzen ari den desplazamenduaren berdina, eta horrek bukle infinitura eraman lezake. _nx_dns_resource_name_real_size_calculate funtzioan punteroa aurrera begira egin liteke, eta ez dago konprobaziorik paketearen bufferraren mugetatik kanpo. Oraindik ez da ahultasun horretarako identifikatzailerik esleitu.

Ahultasun horien xehetasunak txosten teknikoan azaltzen dira, hemen aurkeztuko dira: Black Hat Asia 2021.

Etiketak: Eguneratzea, Komunikazioak, DNS, IoT, Ahultasuna.

2021eko apirileko SAP segurtasunaren eguneratzea

Argitalpen data: 2021/04/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa;
- SAP Commerce, 1808, 1811, 1905, 2005 eta 2011 bertsioak;
- SAP NetWeaver AS JAVA (MigrationService), 7.10, 7.11, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
- SAP NetWeaver Master Data Management, bertsioak: 710 eta 710.750;
- SAP Solution Manager, 7.20 bertsioa;
- SAP NetWeaver AS for ABAP, bertsioak: 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731 y 2011_1_752, 2020, 731, 740, 750 eta 7.30;
- SAP S4 HANA (SAP Landscape Transformation), bertsioak: 101, 102, 103, 104 eta 105;
- SAP Setup, 9.0 bertsioa;
- SAP NetWeaver AS for JAVA (Telnet Commands):
  - ENGINEAPI, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
  - ESP_FRAMEWORK, 7.10, 7.20, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
  - SERVERCORE, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
  - J2EE-FRMW, 7.10, 7.20, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
- SAP NetWeaver AS for JAVA (Applications based on HTMLB for Java):
  - EP-BASIS, 7.10, 7.11, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
  - FRAMEWORK-EXT, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
  - FRAMEWORK, 7.10 eta 7.11 bertsioak;
- SAP NetWeaver AS for JAVA (Customer Usage Provisioning Servlet), 7.31, 7.40 eta 7.50 bertsioak;
- SAP Process Integration, 7.10, 7.20, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
- SAP Manufacturing Execution, 15.1, 15.2, 15.3 eta 15.4 bertsioak;
- SAP NetWeaver Application Server Java (Applications based on Web Dynpro Java), 7.00, 7.10, 7.11, 7.20, 7.30, 731, 7.40 eta 7.50 bertsioak;
- SAP Focused RUN, 200 eta 300 bertsioak;
- SAP NetWeaver AS for JAVA (HTTP Service), bertsioak: 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50;
- SAP Fiori Apps 2.0 for Travel Management in SAP ERP, 608 bertsioa.

Azalpena:

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

Konponbidea:

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

Xehetasunak:

SAPek, segurtasun-partxeen hileroko komunikazioan, 14 segurtasun-ohar eta aurreko oharren 5 eguneratze egin ditu. Horietako 3 larritasun kritikokoak dira, 5 handikoak eta 11 tartekoak.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- XSS motako 2 ahultasun (Cross-Site Scripting),
- Zerbitzu ukapenaren inguruko ahultasun bat (DoS).
- Informazioa argitaratze motako ahultasun 5.
- Egiaztatzea konprobatze faltaren 5 ahultasun.
- Kodearen urrutiko exekuzioaren ahultasun bat.
- Beste motaren bateko 5 ahultasun.

Segurtasun ohar nabarmenenak honakoen ingurukoak dira:

- SAP Commerce. Urruneko kodearen exekuzioa zuzendu da; horren bidez, erasotzaile batek, baimenduta egon gabe, arauen motorraren scripting gaitasunak baliatu litzake, jatorrizko arauetan kode maltzurra injektatzeko, eta, horrela, kodearen urruneko exekuzioa bideratzeko. Ahultasun horretarako, CVE-2021-27602 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2021-21481, CVE-2021-21482, CVE-2021-21483, CVE-2020-26832, CVE-2021-27608, CVE-2021-21485, CVE-2021-27598, CVE-2021-27603, CVE-2021-27599, CVE-2021-27604, CVE-2021-27600, CVE-2021-27601, CVE-2021-21491, CVE-2021-27609, CVE-2021-21492 eta CVE-2021-27605.

Etiketak: Eguneratzea, SAP, Ahultasuna

5.7.1 Segurtasun eguneratzea WordPress-erako

Argitalpen data: 2021/04/15

Garrantzia: Altua

Kaltetutako baliabideak:

WordPress, 5.7.1 bertsioaren aurreko guztiak.

Azalpena:

WordPress-en azken bertsioa argitaratu da; 26 akats eta 2 segurtasun arazo konpondu dira horren bidez.

Konponbidea:

5.7.1 bertsiora eguneratzea.

Xehetasunak:

Segurtasun-zuzenketek honako ahultasunak zuzentzen dituzte:

- XXE (XML External Entity) PHP 8 sistemari eragiten dion multimedia liburutegian.
- Datuak erakusgai REST API sisteman.

Etiketak: Eguneratzea, CMS, PHP, Ahultasuna.

Hainbat ahultasun GitLab eta Ruby sistemetan

Argitalpen data: 2021/04/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- GitLab Community Edition (CE)/Enterprise Edition (EE), 11.9 bertsioa eta ostekoak.
- Ruby, bertsioak:
  - 2.5.8 edo aurrekoak,
  -
  - 2.6.7 edo aurrekoak,
- 2.7.2 edo aurrekoak,
- 3.0.1 edo aurrekoak.

-
- REXML gem, 3.2.4 bertsioa edo aurrekoak.

Azalpena:

vakzz eta Juho Nurminen, ikertzaileek, HackerOne delakoaren *bug bount*y programaren bidez, GitLab eta REXML sistemei eragiten dieten 2 ahultasun kritiko antzeman dituzte. Motak: kodearen urruneko exekuzioa (RCE) eta XML dokumentuen konbertsioa, hurrenez hurren.

Konponbidea:

Eguneratzea:

- GitLab CE/EE, bertsioak: 13.10.3, 13.9.6 eta 13.8.8.
- REXML gem 3.2.5 edo osteko bertsio batera.

Xehetasuna:

- GitLab CE/EE ahultasun bat antzeman da. Horren bidez, artxibo analizatzaile batera pasatzen ziren artxiboak ez ziren behar den moduan balioztatzen, beraz, komandoen urruneko exekuzioa ematen zen.
-
- Bereziki diseinatutako XML dokumentu bat partxeatu eta serializatzean, REXML gem (Rubyrekin ere barne hartzen dena) sistemak XML dokumentu oker bat sortu lezake, jatorrizkoaren egitura desberdinarekin. Ahultasun horretarako, CVE-2021-28965 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Kodearen urruneko exekuzioa Juniper produktuen overlayd zerbitzuan

Argitalpen data: 2021/04/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Juniper Networks Junos OS, bertsioak:
  - 15.1, anteriores a 15.1R7-S9;
  - 17.3, anteriores a 17.3R3-S11;
  - 17.4, anteriores a 17.4R2-S13 y 17.4R3-S4;
  - 18.1, anteriores a 18.1R3-S12;
  - 18.2, anteriores a 18.2R2-S8 y 18.2R3-S7;
  - 18.3, anteriores a 18.3R3-S4;
  - 18.4, anteriores a 18.4R1-S8, 18.4R2-S7 y 18.4R3-S7;
  - 19.1, anteriores a 19.1R2-S2 y 19.1R3-S4;
  - 19.2, anteriores a 19.2R1-S6 y 19.2R3-S2;
  - 19.3, anteriores a 19.3R3-S1;
  - 19.4, anteriores a 19.4R2-S4 y 19.4R3-S1;
  - 20.1, anteriores a 20.1R2-S1 y 20.1R3;
  - 20.2, anteriores a 20.2R2, 20.2R2-S1 y 20.2R3;
  - 20.3, anteriores a 20.3R1-S1.
  - 15.1 bertsioak, 15.1R7-S9ren aurrekoak;
  - 17.3 bertsioak, 17.3R3-S11en aurrekoak;
  - 17.4 bertsioak, 17.4R2-S13 eta 17.4R3-S4ren aurrekoak;
  - 18.1 bertsioak, 18.1R3-S12ren aurrekoak;
  - 18.2 bertsioak, 18.2R2-S8 eta 18.2R3-S7ren aurrekoak;
  - 18.3 bertsioak, 18.3R3-S4ren aurrekoak;
  - 18.4 bertsioak, 18.4R1-S8, 18.4R2-S7 eta 18.4R3-S7ren aurrekoak;

- 19.1 bertsioak, 19.1R2-S2 eta 19.1R3-S4ren aurrekoak;
- 19.2 bertsioak, 19.2R1-S6 eta 19.2R3-S2ren aurrekoak;
- 19.3 bertsioak, 19.3R3-S1en aurrekoak;
- 19.4 bertsioak, 19.4R2-S4 eta 19.4R3-S1en aurrekoak;
- 20.1 bertsioak, 20.1R2-S1 eta 20.1R3ren aurrekoak;
- 20.2 bertsioak, 20.2R2, 20.2R2-S1 eta 20.2R3ren aurrekoak;
- 20.3 bertsioa, 20.3R1-S1en aurrekoak.

Azalpena:

Bufferraren tamainaren balioztatze desegokiaren (overload zerbitzuak) motako ahultasun bat argitaratu da. Horren bidez, erasotzaile batek zerbitzu ukapena edota kodearen urruneko exekuzioa bideratu ahal izango lituzke.

Konponbidea:

- Honako bertsioetara eguneratzea:
  - 15.1R7-S9;
  - 17.3R3-S11;
  - 17.4R2-S13 eta 17.4R3-S4;
  - 18.1R3-S12;
  - 18.2R2-S8 eta 18.2R3-S7;
  - 18.3R3-S4;
  - 18.4R1-S8, 18.4R2-S7 eta 18.4R3-S7;
  - 19.1R2-S2 eta 19.1R3-S4;
  - 19.2R1-S6 eta 19.2R3-S2;
  - 19.3R3-S1;
  - 19.4R2-S4 eta 19.4R3-S1;
  - 20.1R2-S1 eta 20.1R3;
  - 20.2R2, 20.2R2-S1 eta 20.2R3;
  - 20.3R1-S1.

Xehetasuna:

Bufferraren tamainaren balioztatze desegokiaren motako ahultasun baten bidez (overlayd zerbitzuan), urruneko erasotzaile batek, baimenik gabe, bereziki diseinatutako paketeak bidal litzake gailura, zerbitzuaren ukapen partziala (DoS) edota kodearen urruneko exekuzioa eraginez. Ahultasun horretarako, CVE-2021-0254 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Kodearen urruneko exekuzioa Pulse Connect Secure sisteman

Argitalpen data: 2021/04/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Pulse Connect Secure, 9.0R3 bertsioa eta ostekoa.

Azalpena:

Pulse Connect Secure (PCS) sisteman ahultasun bat antzeman da. Horren bidez, erasotzaile batek, baimenik behar izan gabe, artxibo arbitrarioen urruneko exekuzioa eragin lezake Pulse Connect Secure-ren lotura-atean. Ahultasun horrek arrisku handia dakar eta aktiboki baliatzen ari dira.

Konponbidea:

Pulse Connect Secure 9.1R.11.4 bertsiora eguneratzea, eskuragarri dagoenean.

Bitartean, Pulse Secure sistemak gomendatzen du Workaround-2104.xml artxiboa inportatzea, PCS instantzietan kaltetutako ezaugarri multzoak desaktibatzeko: Windows File Share Browser eta Pulse Secure Collaboration.

Xehetasuna:

Windows File Share Browser eta Pulse Connect Secure-ren Pulse Secure Collaboration funtzioek agerian utzitako ahultasun baten bidez, urruneko erasotzaile batek, baimenik gabe, kode arbitrarioa exekuta lezake Pulse Connect Secure sistemaren lotura ahularen ate-sisteman. Ahultasun horretarako, CVE-2021-22893 identifikatzailea esleitu da.

Etiketak: 0day, Ahultasuna

Hainbat 0day ahultasun SonicWall Email Security sisteman

Argitalpen data: 2021/04/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Email Security (ES), bertsio hauek: 10.0.1, 10.0.2, 10.0.3 eta 10.0.4 egungora arte;
-
- Hosted Email Security (HES), bertsioak: 10.0.1, 10.0.2, 10.0.3 eta 10.0.4, egungora arte.

SonicWall Email Security sistemaren 7.0.0-9.2.2 bertsioak ahultasun horien mende daude. Hala ere, bertsio horiek beren bizitza erabilgarriaren amaierara heldu dira (EOL) eta ez dute babesik jasotzen.

Azalpena:

FireEye Mandiant Managed Defense taldeak hiru 0day ahultasun antzeman ditu SonicWall Email Security (ES) sisteman; bat larritasun kritikokoa eta beste biak tarteko larritasunekoak. Aktiboki baliatzen ari dira ahultasun horiek, sarbide administratiboa lortzeko eta kodearen exekuzioa burutzeko, beraz, hardware gailuak, gailu birtualak edota SonicWall Email Securityren software instalazioak (Microsoft Windows Server sisteman) erabiltzen dituzten erakundeek berehala eguneratu behar dute zuzentzen dituen bertsiora.

Konponbidea:

Eguneratzea:

- Email Security 10.0.9.6173 (Windows);
-
- Email Security 10.0.9.6177 (Hardware eta ESXi Virtual Appliance);
- Hosted Email Security 10.0.9.6173 (automatikoki partxeatua).

Xehetasuna:

- SonicWall Email Security aplikazioak egiaztatze kontrol-panela dauka, administrazio gaitasunak emateko. Ahultasun hori dela eta, bereziki diseinatutako XML dokumentua daukan erasotzaile batek HTTP eskaerak egin litzake aplikaziora, eta role.ouadmin kontu bat sortu. Hori, era berean, aplikazioan administrari bezala sartzeko erabil liteke. Ahultasun kritiko horretarako, CVE-2021-20021 identifikatzailea esleitu da.
-
- Erabiltzailearen web interfazera igotako ZIP artxiboen balioztatze faltaren ondorioz, erasotzaile batek kode exekutagarria duten artxibo maltzurrak eta webshell delakoak igo litzake kokapen arbitrarioetan. Ahultasun horretarako, CVE-2021-20022 identifikatzailea esleitu da.
- Panel administratiboan integratutako branding delakoaren egiaztatzearen bidez, erasotzaile batek host-aren artxibo arbitrarioak berreskuratu litzake, bereziki diseinatutako http eskaerak baliabide zehatz batera bidaliz. Ahultasun horretarako, CVE-2021-20023 identifikatzailea esleitu da.

Etiketak: 0day, Eguneratzea, Komunikazioak, Microsoft, Birtualizazioa, Ahultasuna.

XSS Ahultasuna TIBCO Administrator sisteman

Argitalpen data: 2021/04/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Produktu hauen 5.11.0, 5.11.1, 5.10.2 bertsioak eta aurrekoak:

- TIBCO Administrator - Enterprise Edition;
- TIBCO Administrator - Enterprise Edition Distribution, TIBCO Silver Fabric-erako ;
- TIBCO Administrator - Enterprise Edition, z/Linux-erako;
- TIBCO Runtime Agent;
- TIBCO Runtime Agent, z/Linux-erako;

administration GUI osagaia.

Azalpena:

TIBCOk ahultasun kritiko baten berri eman du, biltegiratutako XSS motakoa. Hori baliatuz, erasotzaile batek sarbide administratibo osoa izan lezake kaltetutako sistemara.

Konponbidea:

Kaltetutako produktuak 5.10.3, 5.11.2 edota osteko bertsioetara eguneratzea, kaltetutako bertsioari dagokionaren arabera.

Xehetasuna:

Unix-en oinarritutako sistemetan ahultasun bat dago, eta, horren bidez, erasotzaile batek, baimen beharrik gabe, ingeniaritza soziala egin ahalko lioke sarerako sarbidea duen erabiltzaile bati, biltegiratutako XSS motako eraso bat exekutatzeko, kaltetutako sistemara bideratuta. Ahultasun horretarako, CVE-2021-28827 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Linux, Ahultasuna

Hainbat ahultasun Arubaren ClearPass sisteman

Argitalpen data: 2021/04/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- ClearPass 6.9.x, 6.9.5 bertsioaren aurreko guztiak;
- ClearPass 6.8.x, 6.8.9 bertsioaren aurreko guztiak;
- ClearPass 6.9.x, 6.7.14 eta 6.7.14-HF1 bertsioaren aurreko guztiak.

Azalpena:

Hainbat ikertzailek 10 ahultasunen berri eman dute: bat larritasun kritikokoa eta beste 9 larritasun handikoak. Horien bidez, urruneko erasotzaile batek, baimenik gabe, kode arbitrarioa exekuta lezake, zerbitzuaren ukapena eragin, informazio konfidentziala eskuratu edo kredentzialak lapurtu, hurrenez hurren.

Konponbidea:

Eguneratzea:

- ClearPass 6.9.x 6.9.5 bertsiora edo osteko batera;
- ClearPass 6.8.x 6.8.9 bertsiora edo osteko batera;
- ClearPass 6.7.x, 6.7.14 eta 6.7.14-HF1 bertsiora edo osteko batera, hurrenez hurren.

Xehetasuna:

ClearPass administrazio webguneko interfazeko SSRF (Server Side Request Forgery) motako ahultasun baten bidez, urruneko erasotzaile batek, baimenik lortu gabe, kode arbitrarioa exekuta lezake ClearPass host-ean. Larritasun handiko ahultasun horretarako CVE-2021-29145 identifikatzailea esleitu da.

Gainerako ahultasunetarako, identifikatzaile hauek esleitu dira: CVE-2021-29139, CVE-2021-29142, CVE-2021-29146, CVE-2021-29140, CVE-2020-7123, CVE-2021-29138, CVE-2020-29147, CVE-2021-29141 eta CVE-2021-29144.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Eguneraketa kritikoak Oraclen (2021eko apirila)

Argitalpen data: 2021/04/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite, 3.5 eta 3.6 bertsioak;
- Agile Product Lifecycle Management Integration Pack for SAP: Design to Release, 3.5 eta 3.6 bertsioak;
- Enterprise Manager Base Platform, 13.4.0.0 bertsioa;
- Enterprise Manager for Fusion Middleware, 12.2.1.4 eta 13.4.0.0 bertsioak;
- Enterprise Manager for Virtualization, 13.4.0.0 bertsioa;
- Enterprise Manager Ops Center, 12.4.0.0 bertsioa;
- FMW Platform, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak;
- Hyperion Analytic Provider Services, 11.1.2.4 eta 12.2.1.4 bertsioak;
- Hyperion Financial Management, 11.1.2.4 bertsioa;
- Instantis EnterpriseTrack, 17.1, 17.2 eta 17.3 bertsioak;
- JD Edwards EnterpriseOne Orchestrator, 9.2.5.3aren aurreko bertsioak;
- JD Edwards EnterpriseOne Tools, 9.2.4.0 eta 9.2.5.3 bertsioen aurreko guztiak;
- JD Edwards World Security, A9.4 bertsioa;
- MySQL Cluster, 8.0.23 bertsioa eta aurrekoak;
- MySQL Enterprise Monitor, 8.0.23 bertsioa eta aurrekoak;
- MySQL Server, 5.7.33 bertsioa eta aurrekoak, eta 8.0.23 bertsioa eta aurrekoak;
- MySQL Workbench, 8.0.23 bertsioa eta aurrekoak;
- Oracle Advanced Supply Chain Planning, 12.1 eta 12.2 bertsioak;
- Oracle Agile PLM, 9.3.3, 9.3.5 eta 9.3.6 bertsioak;
- Oracle API Gateway, 11.1.2.4.0 bertsioa;
- Oracle Application Express, 20.2 bertsioaren aurreko guztiak;
- Oracle Application Testing Suite, 13.3.01 bertsioa;
- Oracle BAM, 11.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak;
- Oracle Banking Platform, bertsioak: 2.4.0, 2.6.2, 2.7.0, 2.7.1, 2.8.0, 2.9.0 eta 2.10.0;
- 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 Cloud Infrastructure Storage Gateway, 1.4 bertsioaren aurreko guztiak;
- 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 Commerce Guided Search, bertsioak: 11.3.0, 11.3.1 eta 11.3.2;
- Oracle Commerce Merchandising, bertsioak: 0, 11.0.0, 11.1, 11.2.0, 11.3.0, 11.3.1 eta 11.3.2;
- Oracle Communications Application Session Controller, 3.9m0p3 bertsioa;
- Oracle Communications Calendar Server, 8.0 bertsioa;
- Oracle Communications Contacts Server, 8.0 bertsioa;
- Oracle Communications Converged Application Server ? Service Controller, 6.2 bertsioa;
- Oracle Communications Design Studio, 7.4.2 bertsioa;
- Oracle Communications Interactive Session Recorder, 6.3 eta 6.4 bertsioak;
- Oracle Communications Messaging Server, 8.0.2, 8.1 eta 8.1.0 bertsioak;
- Oracle Communications MetaSolv Solution, 6.3.0 eta 6.3.1 bertsioak;
- Oracle Communications Performance Intelligence Center Software, 10.4.0.2 eta 10.4.0.3 bertsioak;
- Oracle Communications Services Gatekeeper, 6.0, 6.1, 7.0 bertsioak;
- Oracle Communications Session Border Controller, Cz8.2, Cz8.3 eta Cz8.4 bertsioak;
- Oracle Communications Session Router, Cz8.2, Cz8.3 eta Cz8.4 bertsioak;
- Oracle Communications Subscriber-Aware Load Balancer, Cz8.2, Cz8.3 eta Cz8.4 bertsioak;
- Oracle Communications Unified Inventory Management, 7.3.4, 7.3.5, 7.4.0 eta 7.4.1 bertsioak;
- Oracle Communications Unified Session Manager, SCz8.2.5 bertsioa;
- 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 Studio, 3.2.0.0 bertsioa;
- Oracle Enterprise Communications Broker, PCZ3.1, PCZ3.2 eta PCZ3.3 bertsioak;
- Oracle Enterprise Repository, 11.1.1.7.0 bertsioa;
- Oracle Enterprise Session Border Controller, Cz8.2, Cz8.3 eta Cz8.4 bertsioak;
- Oracle Financial Services Analytical Applications Infrastructure, 8.0.6tik 8.1.0era bitarteko bertsioak;
- Oracle FLEXCUBE Direct Banking, 12.0.2 eta 12.0.3 bertsioak;
- Oracle FLEXCUBE Private Banking, 12.0.0 eta 12.1.0 bertsioak;
- Oracle Fusion Middleware, 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak;
- Oracle Fusion Middleware MapViewer, 12.2.1.4.0 bertsioa;
- Oracle Global Lifecycle Management OPatch, 12.2.0.1.22 bertsioaren aurreko guztiak;
- Oracle GraalVM Enterprise Edition, 19.3.5, 20.3.1.2 eta 21.0.0.2 bertsioak;
- Oracle Graph Server and Client;
- Oracle Health Sciences Empirica Signal, 9.0 eta 9.1 bertsioak;
- Oracle Health Sciences Information Manager, 3.0.0tik a la 3.0.2ra bitarteko bertsioak;
- Oracle Healthcare Foundation, bertsioak: 7.1.5, 7.2.2, 7.3.0, 7.3.1 eta 8.0.1;
- Oracle Hospitality Cruise Shipboard Property Management System, 20.1.0 bertsioa;
- Oracle Hospitality Inventory Management, 9.1.0 bertsioa;
- Oracle Hospitality OPERA 5, 5.5 eta 5.6 bertsioak;
- Oracle Hospitality RES 3700, 5.7.0tik 5.7.6ra bitarteko bertsioak;
- Oracle HTTP Server, bertsioak: 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle Identity Manager Connector, 11.1.1.5.0 bertsioa;
- Oracle iLearning, 6.2 eta 6.3 bertsioa;
- Oracle Insurance Data Gateway, 1.0.2.3 bertsioa;
- Oracle Java SE, 7u291, 8u281, 11.0.10 eta 16 bertsioak;
- Oracle Java SE Embedded, 8u281 bertsioa;
- Oracle NoSQL Database, 20.3aren aurreko bertsio guztiak;
- Oracle Outside In Technology, 8.5.5 bertsioa;
- Oracle Platform Security for Java, bertsioak: 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle Rapid Planning, 12.1.3 bertsioa;
- Oracle REST Data Services, 20.4.3.50.1904 bertsioaren aurreko guztiak;
- Oracle Retail Advanced Inventory Planning, 14.1 bertsioa;
- Oracle Retail Assortment Planning, 16.0.3 bertsioa;
- Oracle Retail Back Office, 14.1 bertsioa;
- Oracle Retail Category Management Planning & Optimization, 16.0.3 bertsioa;
- Oracle Retail Back Office, 14.1 bertsioa;
- Oracle Retail EFTLink, bertsioak: 15.0.2, 16.0.3, 17.0.2, 18.0.1, 19.0.1 eta 20.0.0;
- Oracle Retail Insights Cloud Service Suite, 19.0 bertsioa;
- Oracle Retail Item Planning, 16.0.3 bertsioa;
- Oracle Retail Macro Space Optimization, 16.0.3 bertsioa;
- Oracle Retail Merchandise Financial Planning, 16.0.3 bertsioa;
- Oracle Retail Merchandising System, 16.0.3 bertsioa;
- Oracle Retail Point-of-Service, 14.1 bertsioa;
- Oracle Retail Predictive Application Server, 14.1, 15.0 eta 16.0 bertsioak;
- Oracle Retail Regular Price Optimization, 16.0.3 bertsioa;
- Oracle Retail Replenishment Optimization, 16.0.3 bertsioa;
- Oracle Retail Returns Management, 14.1 bertsioa;
- Oracle Retail Sales Audit, 14.0 bertsioa;
- Oracle Retail Size Profile Optimization, 16.0.3 bertsioa;
- Oracle Retail Store Inventory Management, 14.1.3.10, 15.0.3.5 eta 16.0.3.5 bertsioak;
- Oracle Retail Xstore Point of Service, bertsioak: 15.0.4, 16.0.6, 17.0.4, 18.0.3 eta 19.0.2;
- Oracle SD-WAN Aware, 8.2 bertsioa;
- Oracle SD-WAN Edge, 8.2 eta 9.0 bertsioak;
- Oracle Secure Backup;
- Oracle Secure Global Desktop, 5.6 bertsioa;
- Oracle Security Service, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Service Bus, bertsioak: 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle Solaris, 10 eta 11 bertsioak;
- Oracle Spatial Studio, 19.1.0 eta 20.1.1 bertsioen aurrekoak;
- Oracle SQL Developer, 20.4.1.407.6 bertsioaren aurrekoak;
- Oracle Storage Cloud Software Appliance, 16.3.1.4.2 bertsioaren aurreko guztiak;
- Oracle TimesTen In-Memory Database;
- Oracle Utilities Framework, bertsioak: 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0tik 4.3.0.6.0ra, 4.4.0.0.0tik 4.4.0.2.0ra;
- Oracle VM VirtualBox, 6.1.20 bertsioaren aurreko guztiak;
- Oracle WebCenter Portal, 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 bertsioak;
- Oracle WebLogic Server Proxy Plug-In, bertsioak: 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle ZFS Storage Appliance Kit, 8.8 bertsioa;
- OSS Support Tools, 2.12.41en aurreko bertsio guztiak;
- PeopleSoft Enterprise CS Campus Community, 9.2 bertsioa;
- PeopleSoft Enterprise FIN Common Application Objects, 9.2 bertsioa;
- PeopleSoft Enterprise FIN Expenses, 9.2 bertsioa;
- PeopleSoft Enterprise PeopleTools, 8.56, 8.57 eta 8.58 bertsioak;
- PeopleSoft Enterprise PT PeopleTools, 8.56, 8.57 eta 8.58 bertsioak;
- PeopleSoft Enterprise SCM eProcurement, 9.2 bertsioa;
- PeopleSoft Enterprise SCM Purchasing, 9.2 bertsioa;
- Primavera Gateway, 17.12.0tik 17.12.10era bitarteko bertsioak;
- Primavera Unifier, bertsioak: 16.1, 16.2, 17.7tik 17.12ra bitartekoak, 18.8, 19.12 eta 20.12;
- Siebel Applications, 21.2 bertsioa eta aurrekoak.

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.

Xehetasuna:

Eguneratze horrek 390 ahultasun konpontzen ditu, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna Oracleren loturan dagoen Erreferentzien atalean kontsulta daiteke.Etiketak: Eguneratzea, Oracle, Ahultasuna.

Etiketak: Eguneratzea, Oracle, Ahultasuna

Ahultasuna Drupal sistemaren core-an

Argitalpen data: 2021/04/22

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Hauen aurreko bertsioak:

- 9.1.17;
- 9.0.12;
- 8.9.14;
- 7.80.

Azalpena:

Larritasun kritikoko ahultasun baten berri eman da. Drupal sistemaren core-an gertatzen da, eta, horren bidez, cross-site scripting erasoak burutu litezke.

Konponbidea:

Bertsio hauetara eguneratzea: 9.1.7, 9.0.12, 8.9.14, 7.80.

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

Xehetasuna:

Drupal sistemaren core-aren sanitizazio APIak ez du behar den moduan filtratzen cross-site scritpting delakoa, zirkunstantzia batzuetan.

Etiketak: Eguneratzea, CMS, Ahultasuna

Egiaztatze falta FortiWAN sisteman

Argitalpen data: 2021/04/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

FortiWAN, 4.5.7 bertsioa eta aurrekoak.

Descripción:

Azalpena:

Direktorio mugatu baterako ibilbidearen izen mugaketa desegokiaren motako ahultasun baten ondorioz (Relative Path Traversal), urruneko erasotzaile batek, baimenik egiaztatu gabe, sisteman artxiboak ezabatu litzake.

Konponbidea:

- FortiWAN 4.5.8 bertsiora edo osteko batera eguneratzea.
-
- FortiWAN 5.1.1 bertsiora edo osteko batera eguneratzea.

Arintze-neurri moduan, sarbide administratiboa edozein iturritatik baimendu beharrean, konfiantzazko barne host delakoetara mugatu behar da.

Xehetasuna:

Direktorio mugatu baterako ibilbidearen izen mugaketa desegokiaren motako ahultasun baten ondorioz (Relative Path Traversal), urruneko erasotzaile batek, baimena egiaztatu gabe, sisteman artxiboak ezabatu litzake, bereziki diseinatutako POST eskaera bat bidaliz. Zehazki, konfigurazio-artxibo espezifikoak ezabatzeak administrari-pasahitza berrezarriko du, aurrez ezarritako baliora. Ahultasun horretarako, CVE-2021-26102 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Birtualizazioa, Ahultasuna

---

Baliabideen kontrol desegokia Citrix ShareFile

sisteman

Argitalpen data: 2021/04/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Citrix ShareFile biltegiratze-eremuen kontrolatzailea, bertsioak:

- 5.7, 5.7.3 aurrekoak;
- 5.8, 5.8.3 aurrekoak;
- 5.9, 5.9.3 aurrekoak;
- 5.10, 5.10.1 aurrekoak;
- 5.11, 5.11.18 aurrekoak.

Azalpena:

Citrix sistemak larritasun kritikoko ahultasun bat antzeman du, baliabideen kontrol desegokiaren motakoa. ShareFile-ri eragiten dio.

Konponbidea:

Citrix ShareFile honako bertsioetara eguneratzea:

- 5.7.3 eta 5.7ren ostekoak;
- 5.8.3 eta 5.8ren ostekoak;
- 5.9.3 eta 5.9ren ostekoak;
- 5.10.1 eta 5.10en ostekoak;
- 5.11.18 eta 5.11ren ostekoak.

Xehetasuna:

Ahultasun bat antzeman da Citrix ShareFile sistemaren biltegiratze-eremuen kontrolagailuan. Horren bidez, urruneko erasotzaile batek, egiaztatu gabe, biltegiratze-eremuen kontrolagailua konprometitu lezake, betiere, biltegiratze-eremuen kontrolagailuaren sarerako sarbidea badauka. Ahultasun horretarako, CVE-2021-22891 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna

Baimen-egiaztatze falta HPE Edgeline Infrastructure Manager sisteman

Argitalpen data: 2021/04/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HPE Edgeline Infrastructure Manager, 1.22 bertsioaren aurrekoak.

Azalpena:

Tenable Research sistemak HPE sistemari ahultasun kritiko baten berri eman dio. Egiaztatze faltaren motakoa da, urrunetik baliatu daiteke, eta Edgeline Infrastructure Manager produktuari eragiten dio.

Konponbidea:

HPE Edgeline Infrastructure 1.22 edo bertsiora edo osteko batera eguneratzea, fabrikatzailearen laguntza zentrotik.

Xehetasuna:

Urruneko erasotzaile batek ahultasun hori baliatu lezake urruneko egiaztatzea saihesteko; horrela, komando arbitrarioen exekuzioa gerta liteke, sarbide pribilegiatua lortu, zerbitzu ukapena eragin (DoS) eta kaltetutako gailuaren konfigurazioa aldatu. Ahultasun horretarako, CVE-2021-29203 identifikatzailea esleitu da.

Etiketak: Eguneratzea, HP, Ahultasuna

Eguneraketa kritikoak Oraclen (2021eko apirila)

Argitalpen data: 2021/04/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite, 3.5 eta 3.6 bertsioak;
- Agile Product Lifecycle Management Integration Pack for SAP: Design to Release, 3.5 eta 3.6 bertsioak;
- Enterprise Manager Base Platform, 13.4.0.0 bertsioa;
- Enterprise Manager for Fusion Middleware, 12.2.1.4 eta 13.4.0.0 bertsioak;

- Enterprise Manager for Virtualization, 13.4.0.0 bertsioa;
- Enterprise Manager Ops Center, 12.4.0.0 bertsioa;
- FMW Platform, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak;
- Hyperion Analytic Provider Services, 11.1.2.4 eta 12.2.1.4 bertsioak;
- Hyperion Financial Management, 11.1.2.4 bertsioa;
- Instantis EnterpriseTrack, 17.1, 17.2 eta 17.3 bertsioak;
- JD Edwards EnterpriseOne Orchestrator, 9.2.5.3aren aurreko bertsioak;
- JD Edwards EnterpriseOne Tools, 9.2.4.0 eta 9.2.5.3 bertsioen aurreko guztiak;
- JD Edwards World Security, A9.4 bertsioa;
- MySQL Cluster, 8.0.23 bertsioa eta aurrekoak;
- MySQL Enterprise Monitor, 8.0.23 bertsioa eta aurrekoak;
- MySQL Server, 5.7.33 bertsioa eta aurrekoak, eta 8.0.23 bertsioa eta aurrekoak;
- MySQL Workbench, 8.0.23 bertsioa eta aurrekoak;
- Oracle Advanced Supply Chain Planning, 12.1 eta 12.2 bertsioak;
- Oracle Agile PLM, 9.3.3, 9.3.5 eta 9.3.6 bertsioak;
- Oracle API Gateway, 11.1.2.4.0 bertsioa;
- Oracle Application Express, 20.2 bertsioaren aurreko guztiak;
- Oracle Application Testing Suite, 13.3.01 bertsioa;
- Oracle BAM, 11.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak;
- Oracle Banking Platform, bertsioak: 2.4.0, 2.6.2, 2.7.0, 2.7.1, 2.8.0, 2.9.0 eta 2.10.0;
- 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 Cloud Infrastructure Storage Gateway, 1.4 bertsioaren aurreko guztiak;
- 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 Commerce Guided Search, bertsioak: 11.3.0, 11.3.1 eta 11.3.2;
- Oracle Commerce Merchandising, bertsioak: 0, 11.0.0, 11.1, 11.2.0, 11.3.0, 11.3.1 eta 11.3.2;
- Oracle Communications Application Session Controller, 3.9m0p3 bertsioa;
- Oracle Communications Calendar Server, 8.0 bertsioa;
- Oracle Communications Contacts Server, 8.0 bertsioa;
- Oracle Communications Converged Application Server ? Service Controller, 6.2 bertsioa;
- Oracle Communications Design Studio, 7.4.2 bertsioa;
- Oracle Communications Interactive Session Recorder, 6.3 eta 6.4 bertsioak;
- Oracle Communications Messaging Server, 8.0.2, 8.1 eta 8.1.0 bertsioak;
- Oracle Communications MetaSolv Solution, 6.3.0 eta 6.3.1 bertsioak;
- Oracle Communications Performance Intelligence Center Software, 10.4.0.2 eta 10.4.0.3 bertsioak;
- Oracle Communications Services Gatekeeper, 6.0, 6.1, 7.0 bertsioak;
- Oracle Communications Session Border Controller, Cz8.2, Cz8.3 eta Cz8.4 bertsioak;
- Oracle Communications Session Router, Cz8.2, Cz8.3 eta Cz8.4 bertsioak;
- Oracle Communications Subscriber-Aware Load Balancer, Cz8.2, Cz8.3 eta Cz8.4 bertsioak;
- Oracle Communications Unified Inventory Management, 7.3.4, 7.3.5, 7.4.0 eta 7.4.1 bertsioak;
- Oracle Communications Unified Session Manager, SCz8.2.5 bertsioa;
- 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 Studio, 3.2.0.0 bertsioa;
- Oracle Enterprise Communications Broker, PCZ3.1, PCZ3.2 eta PCZ3.3 bertsioak;
- Oracle Enterprise Repository, 11.1.1.7.0 bertsioa;
- Oracle Enterprise Session Border Controller, Cz8.2, Cz8.3 eta Cz8.4 bertsioak;
- Oracle Financial Services Analytical Applications Infrastructure, 8.0.6tik 8.1.0era bitarteko bertsioak;
- Oracle FLEXCUBE Direct Banking, 12.0.2 eta 12.0.3 bertsioak;
- Oracle FLEXCUBE Private Banking, 12.0.0 eta 12.1.0 bertsioak;
- Oracle Fusion Middleware, 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak;
- Oracle Fusion Middleware MapViewer, 12.2.1.4.0 bertsioa;
- Oracle Global Lifecycle Management OPatch, 12.2.0.1.22 bertsioaren aurreko guztiak;
- Oracle GraalVM Enterprise Edition, 19.3.5, 20.3.1.2 eta 21.0.0.2 bertsioak;
- Oracle Graph Server and Client;
- Oracle Health Sciences Empirica Signal, 9.0 eta 9.1 bertsioak;
- Oracle Health Sciences Information Manager, 3.0.0tik a la 3.0.2ra bitarteko bertsioak;
- Oracle Healthcare Foundation, bertsioak: 7.1.5, 7.2.2, 7.3.0, 7.3.1 eta 8.0.1;
- Oracle Hospitality Cruise Shipboard Property Management System, 20.1.0 bertsioa;
- Oracle Hospitality Inventory Management, 9.1.0 bertsioa;
- Oracle Hospitality OPERA 5, 5.5 eta 5.6 bertsioak;
- Oracle Hospitality RES 3700, 5.7.0tik 5.7.6ra bitarteko bertsioak;
- Oracle HTTP Server, bertsioak: 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle Identity Manager Connector, 11.1.1.5.0 bertsioa;
- Oracle iLearning, 6.2 eta 6.3 bertsioa;
- Oracle Insurance Data Gateway, 1.0.2.3 bertsioa;
- Oracle Java SE, 7u291, 8u281, 11.0.10 eta 16 bertsioak;
- Oracle Java SE Embedded, 8u281 bertsioa;
- Oracle NoSQL Database, 20.3aren aurreko bertsio guztiak;
- Oracle Outside In Technology, 8.5.5 bertsioa;
- Oracle Platform Security for Java, bertsioak: 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle Rapid Planning, 12.1.3 bertsioa;
- Oracle REST Data Services, 20.4.3.50.1904 bertsioaren aurreko guztiak;
- Oracle Retail Advanced Inventory Planning, 14.1 bertsioa;
- Oracle Retail Assortment Planning, 16.0.3 bertsioa;
- Oracle Retail Back Office, 14.1 bertsioa;
- Oracle Retail Category Management Planning & Optimization, 16.0.3 bertsioa;
- Oracle Retail Back Office, 14.1 bertsioa;
- Oracle Retail EFTLink, bertsioak: 15.0.2, 16.0.3, 17.0.2, 18.0.1, 19.0.1 eta 20.0.0;
- Oracle Retail Insights Cloud Service Suite, 19.0 bertsioa;
- Oracle Retail Item Planning, 16.0.3 bertsioa;
- Oracle Retail Macro Space Optimization, 16.0.3 bertsioa;
- Oracle Retail Merchandise Financial Planning, 16.0.3 bertsioa;
- Oracle Retail Merchandising System, 16.0.3 bertsioa;
- Oracle Retail Point-of-Service, 14.1 bertsioa;
- Oracle Retail Predictive Application Server, 14.1, 15.0 eta 16.0 bertsioak;
- Oracle Retail Regular Price Optimization, 16.0.3 bertsioa;
- Oracle Retail Replenishment Optimization, 16.0.3 bertsioa;

- Oracle Retail Returns Management, 14.1 bertsioa;
- Oracle Retail Sales Audit, 14.0 bertsioa;
- Oracle Retail Size Profile Optimization, 16.0.3 bertsioa;
- Oracle Retail Store Inventory Management, 14.1.3.10, 15.0.3.5 eta 16.0.3.5 bertsioak;
- Oracle Retail Xstore Point of Service, bertsioak: 15.0.4, 16.0.6, 17.0.4, 18.0.3 eta 19.0.2;
- Oracle SD-WAN Aware, 8.2 bertsioa;
- Oracle SD-WAN Edge, 8.2 eta 9.0 bertsioak;
- Oracle Secure Backup;
- Oracle Secure Global Desktop, 5.6 bertsioa;
- Oracle Security Service, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Service Bus, bertsioak: 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle Solaris, 10 eta 11 bertsioak;
- Oracle Spatial Studio, 19.1.0 eta 20.1.1 bertsioen aurrekoak;
- Oracle SQL Developer, 20.4.1.407.6 bertsioaren aurrekoak;
- Oracle Storage Cloud Software Appliance, 16.3.1.4.2 bertsioaren aurreko guztiak;
- Oracle TimesTen In-Memory Database;
- Oracle Utilities Framework, bertsioak: 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0tik 4.3.0.6.0ra, 4.4.0.0.0tik 4.4.0.2.0ra;
- Oracle VM VirtualBox, 6.1.20 bertsioaren aurreko guztiak;
- Oracle WebCenter Portal, 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 bertsioak;
- Oracle WebLogic Server Proxy Plug-In, bertsioak: 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0;
- Oracle ZFS Storage Appliance Kit, 8.8 bertsioa;
- OSS Support Tools, 2.12.41en aurreko bertsio guztiak;
- PeopleSoft Enterprise CS Campus Community, 9.2 bertsioa;
- PeopleSoft Enterprise FIN Common Application Objects, 9.2 bertsioa;
- PeopleSoft Enterprise FIN Expenses, 9.2 bertsioa;
- PeopleSoft Enterprise PeopleTools, 8.56, 8.57 eta 8.58 bertsioak;
- PeopleSoft Enterprise PT PeopleTools, 8.56, 8.57 eta 8.58 bertsioak;
- PeopleSoft Enterprise SCM eProcurement, 9.2 bertsioa;
- PeopleSoft Enterprise SCM Purchasing, 9.2 bertsioa;
- Primavera Gateway, 17.12.0tik 17.12.10era bitarteko bertsioak;
- Primavera Unifier, bertsioak: 16.1, 16.2, 17.7tik 17.12ra bitartekoak, 18.8, 19.12 eta 20.12;
- Siebel Applications, 21.2 bertsioa eta aurrekoak.

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.

Xehetasuna:

Eguneratze horrek 390 ahultasun konpontzen ditu, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna Oracleren loturan dagoen Erreferentzien atalean kontsulta daiteke.Etiketak: Eguneratzea, Oracle, Ahultasuna.

Etiketak: Eguneratzea, Oracle, Ahultasuna

Ahultasuna Drupal sistemaren core-an

Argitalpen data: 2021/04/22

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Hauen aurreko bertsioak:

- 9.1.17;
- 9.0.12;
- 8.9.14;
- 7.80.

Azalpena:

Larritasun kritikoko ahultasun baten berri eman da. Drupal sistemaren core-an gertatzen da, eta, horren bidez, cross-site scripting erasoak burutu litezke.

Konponbidea:

Bertsio hauetara eguneratzea: 9.1.7, 9.0.12, 8.9.14, 7.80.

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

Xehetasuna:

Drupal sistemaren core-aren sanitizazio APIak ez du behar den moduan filtratzen cross-site scritpting delakoa, zirkunstantzia batzuetan.

Etiketak: Eguneratzea, CMS, Ahultasuna

Egiaztatze falta FortiWAN sisteman

Argitalpen data: 2021/04/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

FortiWAN, 4.5.7 bertsioa eta aurrekoak.

Descripción:

Azalpena:

Direktorio mugatu baterako ibilbidearen izen mugaketa desegokiaren motako ahultasun baten ondorioz (Relative Path Traversal), urruneko erasotzaile batek, baimenik egiaztatu gabe, sisteman artxiboak ezabatu litzake.

Konponbidea:

- FortiWAN 4.5.8 bertsiora edo osteko batera eguneratzea.
-
- FortiWAN 5.1.1 bertsiora edo osteko batera eguneratzea.

Arintze-neurri moduan, sarbide administratiboa edozein iturritatik baimendu beharrean, konfiantzazko barne host delakoetara mugatu behar da.

Xehetasuna:

Direktorio mugatu baterako ibilbidearen izen mugaketa desegokiaren motako ahultasun baten ondorioz (Relative Path Traversal), urruneko erasotzaile batek, baimena egiaztatu gabe, sisteman artxiboak ezabatu litzake, bereziki diseinatutako POST eskaera bat bidaliz. Zehazki, konfigurazio-artxibo espezifikoak ezabatzeak administrari-pasahitza berrezarriko du, aurrez ezarritako baliora. Ahultasun horretarako, CVE-2021-26102 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Birtualizazioa, Ahultasuna

---

Baliabideen kontrol desegokia Citrix ShareFile sisteman

Argitalpen data: 2021/04/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Citrix ShareFile biltegiratze-eremuen kontrolatzailea, bertsioak:

- 5.7, 5.7.3 aurrekoak;
- 5.8, 5.8.3 aurrekoak;
- 5.9, 5.9.3 aurrekoak;
- 5.10, 5.10.1 aurrekoak;
- 5.11, 5.11.18 aurrekoak.

Azalpena:

Citrix sistemak larritasun kritikoko ahultasun bat antzeman du, baliabideen kontrol desegokiaren motakoa. ShareFile-ri eragiten dio.

Konponbidea:

Citrix ShareFile honako bertsioetara eguneratzea:

- 5.7.3 eta 5.7ren ostekoak;
- 5.8.3 eta 5.8ren ostekoak;
- 5.9.3 eta 5.9ren ostekoak;
- 5.10.1 eta 5.10en ostekoak;
- 5.11.18 eta 5.11ren ostekoak.

Xehetasuna:

Ahultasun bat antzeman da Citrix ShareFile sistemaren biltegiratze-eremuen kontrolagailuan. Horren bidez, urruneko erasotzaile batek, egiaztatu gabe, biltegiratze-eremuen kontrolagailua konprometitu lezake, betiere, biltegiratze-eremuen kontrolagailuaren sarerako sarbidea badauka. Ahultasun horretarako, CVE-2021-22891 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna

Baimen-egiaztatze falta HPE Edgeline Infrastructure Manager sisteman

Argitalpen data: 2021/04/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HPE Edgeline Infrastructure Manager, 1.22 bertsioaren aurrekoak.

Azalpena:

Tenable Research sistemak HPE sistemari ahultasun kritiko baten berri eman dio. Egiaztatze faltaren motakoa da, urrunetik baliatu daiteke, eta Edgeline Infrastructure Manager produktuari eragiten dio.

Konponbidea:

HPE Edgeline Infrastructure 1.22 edo bertsiora edo osteko batera eguneratzea, fabrikatzailearen laguntza zentrotik.

Xehetasuna:

Urruneko erasotzaile batek ahultasun hori baliatu lezake urruneko egiaztatzea saihesteko; horrela, komando arbitrarioen exekuzioa gerta liteke, sarbide pribilegiatua lortu, zerbitzu ukapena eragin (DoS) eta kaltetutako gailuaren konfigurazioa aldatu. Ahultasun horretarako, CVE-2021-29203 identifikatzailea esleitu da.

Etiketak: Eguneratzea, HP, Ahultasuna