2020ko Maiatzaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun Citrix-en ShareFile storage zones Controller-en

Argitalpen data: 2020/05/06

Garrantzia: Kritikoa

Kaltetutako baliabideak:

ShareFile storage zones Controller, 5.9.0 eta lehenagoko bertsioak.

Azalpena:

Danske Bank Red-Teamek, Citrixekin lankidetzan, larritasun kritikoko 3 ahultasun aurkitu ditu. Autentifikatu gabeko erasotzaile batek informazioa heda lezake.

Konponbidea:

Storage Zones Controller honako bertsioetara eguneratzea::

- 5.10.0,
- 5.9.1,
- 5.8.1,
- 5.7.1,
- 5.6.1,
- 5.5.1.

Xehetasuna:

Aurkitutako ahultasunak baliatuz, autentifikatu gabeko erasotzaile batek biltegiratze zonen kontrolatzaileak arriskuan jar litzake eta horrela erabiltzaileak ShareFile-n duen informaziora sarbidea lor lezake. Ahultasun horietarako CVE-2020-7473, CVE-2020-8982 eta CVE-2020-8983 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun SaltStack-en Salt-en

Argitalpena data: 2020/05/06

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Salt, 3000.1 bertsioa eta lehenagokoak;
- Salt, 2019.2.3 bertsioa eta lehenagokoak.

Azalpena:

F-Secureren ikertzaileek Salti bere Framework Salti eragiten dioten larritasun kritikoko bi ahultasunen berri eman diote. Urruneko erasotzaile batek autentifikazio kontrolak saihets litzake eta kode arbitrarioa exekutatu sisteman root pribilegioekin.

Konponbidea:

- Salt 3000.X 3000.2 bertsiora edo berriago batera eguneratzea.
- Salt 2019.X 2019.2.4 bertsiora edo berriago batera eguneratzea.

Xehetasuna:

- Salt-master prozesuko ClearFuncs klaseak ez ditu modu egokian baliozkotzen metodoetarako deiak. Urruneko erasotzaile batek metodo batzuetara sarbidea lor lezake autentifikazioa saihestuz. Ahultasun horretarako CVE-2020-11651 identifikatzailea erabili da.
- Salt-master prozesuko ClearFuncs klaseak ahalbidetzen du bideak modu desegokian saneatzen dituzten metodo batzuetara sartzea. Autentifikatutako urruneko erasotzaile batek direktorioetara sarbidea lor lezake. Ahultasun horretarako CVE-2020-11652 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun F5 produktuetan

Argitalpen data: 2020/05/12

Garrantzia: Altua

Kaltetutako baliabideak:

- BIG-IP (APM), honako bertsioak:
  - 15.0.0 - 15.1.0,
  - 14.1.0 - 14.1.2,
  - 13.1.0 - 13.1.3,
  - 12.1.0 - 12.1.5,
  - 11.6.1 - 11.6.5;
- BIG-IP APM Clients, honako bertsioak:
  - 7.1.5 - 7.1.9.

Azalpena:

Red Team/CERT Société Générale-ko Juliette Chapalain-ek bi ahultasun aurkitu ditu, biak larritasun altukoak, F5-ek Windowserako duen BIG-IP Edge Client produktuari eragiten diotenak, fitxategi eta karpeten baimen ez-nahiko eta aldez aurretik askatutako memoriaren erabilpen erakoak.

Konponbidea:

BIG-IP APMren 13.1.0 eta ondorengo bertsioetan, APM Clients-en osagaiak BIG-IP software-tik aparte egunera daitezke, hemen adierazten den moduan: *K52547540: Updating BIG-IP Edge Client for the BIG-IP APM system* eta *K13757: BIG-IP Edge Client version matrix*.

Xehetasuna:

- BIG-IP Edge Client Windows Installer Serviceren aldi baterako karpetak baimen desegokiak dituzten fitxategi eta karpetak ditu, eta sinatutako .exe eta MSI fitxategiak exekutatzea ahalbidetzen du. Hori baliatuz pribilegiorik gabeko erabiltzaile batek pribilegioen eskalatzea egin lezake Windowsen bezeroan. Ahultasun horretarako CVE-2020-5896 identifikatzailea erreserbatu da.
- BIG-IP Edge Client Windows ActiveX-k duen aldez aurretik askatutako memoria erako ahultasuna baliatuz, erasotzaile batek akatsak eragin litzake nabigatzailearen memorian, edo kodea exekuta lezake nabigatzailetik, asmo gaiztoko webgune bat sortuz eta Internet Explorer nabigatzailean kargatuz, BIG-IP Edge Client-en erabiltzaileek erabiltzen dutena. Ahultasun horretarako CVE-2020-5897 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Microsoften 2020ko maiatzeko segurtasun buletina

Argitalpen data: 2020/05/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows;
- Microsoft Edge (EdgeHTML oinarritua);
- Microsoft Edge (Chromium oinarritua);
- ChakraCore;
- Internet Explorer;
- Microsoft Office, Microsoft Office Services etea Web Apps;
- Windows Defender;
- Visual Studio;
- Microsoft Dynamics;
- .NET Framework;
- .NET Core;
- Power BI.

Azalpena:

Segurtasun eguneraketei buruzko Microsoften maiatzeko argitalpenean 111 ahultasun jaso dira, 16 kritiko gisa sailkatu dira eta 95 garrantzitsu gisa.

Konponbidea:

Dagozkien segurtasun eguneraketak instalatzea. Microsoften webgunean eguneraketa horiek egiteko metodo ezberdinei buruzko argibideak daude.

Xehetasuna:

Argitaratutako ahultasun motak honako hauek dira:

- kodearen urruneko exekuzioa,
- pribilegioen eskalatzea,

- zerbitzuaren ukapena,
- informazioaren zabalkundea,
- identitatea ordeztea (spoofing),
- segurtasun murrizpenak saihestea.

Etiketak: Eguneraketa, Microsoft, Ahultasuna, Nabigatzailea, Ahultasuna

---

SAPen 2020ko maiatzeko segurtasun eguneraketa

Argitalpen data: 2020/05/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Application Server ABAP, 2008_1_46C, 2008_1_620, 2008_1_640, 2008_1_700, 2008_1_710 eta 740 bertsioak;
- SAP Business Client, 6.5 bertsioa;
- SAP Business Objects Business Intelligence Platform (Live Data Connect), 1.0, 2.0 eta 2.x bertsioak;
- SAP Adaptive Server Enterprise (Backup Server), 16.0 bertsioa;
- SAP Business Objects Business Intelligence Platform (CrystalReports WebForm Viewer), 4.1 eta 4.2 bertsioak;
- SAP Adaptive Server Enterprise(Cockpit), 16.0 bertsioa;
- SAP Adaptive Server Enterprise, 16.0 bertsioa;
- SAP Application Server ABAP, 2008_1_46C, 2008_1_620, 2008_1_640, 2008_1_700, 2008_1_710 eta 740 bertsioak;
- SAP Business Client, 6.5 bertsioa;
- SAP Business Objects Business Intelligence Platform (Live Data Connect), 1.0, 2.0 eta 2.x bertsioak;
- SAP Adaptive Server Enterprise (Backup Server), 16.0 bertsioa;
- SAP Business Objects Business Intelligence Platform (CrystalReports WebForm Viewer), 4.1 eta 4.2 bertsioak;
- SAP Adaptive Server Enterprise (Cockpit), 16.0 bertsioa;
- SAP Adaptive Server Enterprise, 16.0 bertsioa;
- SAP Adaptive Server Enterprise (XP Server on Windows Platform), 15.7 eta 16.0 bertsioak;
- SAP Master Data Governance, honako bertsioak: S4CORE 101; S4FND 102, 103 eta 104; SAP_BS_FND 748;
- SAP Adaptive Server Enterprise (Web Services), 15.7 eta 16.0 bertsioak;
- SAP Business Client, 7.0 bertsioa;
- SAP Adaptive Server Enterprise, 16.0 bertsioa;
- SAP Business Objects Business Intelligence Platform, 4.2 bertsioa;
- SAP Adaptive Server Enterprise, 15.7 eta 16.0 bertsioak;
- SAP Enterprise Threat Detection, 1.0 eta 2.0 bertsioak;
- SAP Master Data Governance, 748, 749, 750, 751, 752, 800, 801, 802, 803 eta 804 bertsioak;
- SAP Business Objects Business Intelligence Platform(CMC eta BI launchpad), 4.2 bertsioa;
- SAP Plant Connectivity, 15.1, 15.2, 15.3 eta 15.4 bertsioak;
- SAP NetWeaver AS ABAP (Web Dynpro ABAP), honako bertsioak: SAP_UI 750, 752, 753 eta 754; SAP_BASIS 700, 710, 730, 731 eta 804;
- SAP Business Objects Business Intelligence Platform, 4.1, 4.2 eta 4.3 baino lehenagoko bertsioak;
- SAP Business Objects Business Intelligence Platform, 4.1, 4.2 eta 4.3 baino lehenagoko bertsioak;
- SAP Identity Management, 8.0 bertsioa.

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:

SAPek segurtasun partxeei buruz argitaratzen duen hileroko komunikatuan 18 segurtasun ohar eta 4 eguneraketa eman ditu ezagutzera. Horietatik 6 larritasun kritikokoak dira, 4 larritasun altukoak eta 12 larritasun ertainekoak.

Argitaratutako ahultasun motak honako hauek dira:

- kodearen injekzio erako 3 ahultasun,
- Cross-Site Scripting erako 2 ahultasun,
- zerbitzuaren ukapen erako 2 ahultasun;
- informazioaren zabalkunde erako 3 ahultasun,
- autentifikazio faltako ahultasun 1,
- autentifikazioaren egiaztapen gabeziako 3 ahultasun,
- SQL injection erako 3 ahultasun,
- beste era batzuetako 7 ahultasun.

Segurtasun ohartarazpen nagusiak honi buruzkoak dira:

- Kodea dinamikoki sortzen duen eta urrunetik gaituta izan den funtzio modulu batean sarrera datuak modu nahikoan ez baliozkotzea baliatuz, erasotzaile batek Solution Manager (SolMan) sistema batera konektatuta dagoen SAP NWren edozein ABAP sistemaren kontrol osoa har lezake. Ahultasun horretarako CVE-2020-6262 identifikatzailea erabili da.
- SAP Business Objects Business Intelligence Platform-en (Live Data Connect) 1.0, 2.0 eta 2.x bertsioetan autentifikazioaren egiaztapen falta baliatuz, erasotzaile batek kudeaketaren kontsola nagusian pasahitzik gabe sar liteke, aplikazioen BIPRWS zerbitzaria ziurtagiri bereziren batekin babestuta egongo ez balitz. Ahultasun horretarako CVE-2020-6242 identifikatzailea erabili da.
- SAP Adaptive Server Enterpriseren (Backup Server) 16.0 bertsioak ez ditu egiten beharrezkoak diren baliozkotze egiaztapenak erabiltzaile autentifikatu baten kasuan, DUMP edo LOAD komandoa exekutatzen den bitartean. Hori baliatuz erasotzaile batek kode arbitrarioak exekuta litzake edo kodeak injektatu. Ahultasun horretarako CVE-2020-6248 identifikatzailea erabili da.
- Egoera batzuetan SAP Adaptive Server Enterprise (Cockpit) baliatuz, sare lokalera sarbidea lukeen erasotzaile batek informazio sentikorra eta konfidentziala eskura lezake, eta horrela erabiltzaile kontuen kredentzialak eskura litzake, sistemako datuak manipulatu edo sistemaren eskuragarritasunean eragin. Ahultasun horretarako CVE-2020-6252 identifikatzailea erabili da.

Gainerako ahultasunetarako erabilitako identifikatzaileak honako hauek dira: CVE-2020-6219, CVE-2020-6241, CVE-2020-6243, CVE-2020-6249, CVE-2020-6253, CVE-2020-6244, CVE-2020-6250, CVE-2020-6245, CVE-2020-6259, CVE-2020-6254, CVE-2020-6256, CVE-2020-6257, CVE-2020-6240, CVE-2019-0352, CVE-2019-0352 eta CVE-2020-6258.

Etiketak: Eguneraketa, SAP, Ahultasuna

Hainbat ahultasun Palo Alto Networks-en produktuetan

Argitalpen data: 2020/05/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- PAN-OS 9.1, 9.1.1 baino lehenagoko bertsioak;
- PAN-OS 9.0, 9.0.7 baino lehenagoko bertsioak;
- PAN-OS 8.1, 8.1.14 baino lehenagoko bertsioak;
- PAN-OS 8.0, bertsio guztiak;
- PAN-OS 7.1, bertsio guztiak.

Azalpena:

Palo Alto Networks-ek 16 segurtasun ohartarazpen argitaratu ditu produktuen bere segurtasun zentroan, 1 larritasun kritikokoa eta 15 larritasun altukoak.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- PAN-OS 9.1, 9.1.1 bertsiora edo berriago batera;
- PAN-OS 9.0, 9.0.7 bertsiora edo berriago batera;
- PAN-OS 8.1, 8.1.14 bertsiora edo berriago batera.

PAN-OS 7.1en zerbitzua luzatuta dago 2020ko ekainaren 30a arte, eta soilik hartzen da kontuan segurtasuneko ahultasun kritikoen kasuan.

PAN-OS 8.0 bere bizitza erabilgarriaren amaierara iritsi da, eta fabrikatzailearen segurtasun produktuen garantia polizek ez dute babesten.

Xehetasuna:

Erabiltzaile batek aipatutako ahultasunak baliatuko balitu, kaltetutako produktuetan honako ekintza hauek egin litzake:

- pribilegioen eskalatzea,
- PAN-OSra administratzaile modura sartu,
- erabiltzaile aktiboaren saioa arriskuan jarri,
- kode arbitrarioa exekutatu root pribilegioekin,
- sistema eragileko komandoak exekutatu root pribilegioekin,
- sistemako fitxategi arbitrarioak ezabatu,
- sistemaren integritatea arriskuan jarri,
- zerbitzuaren ukapena (DoS),
- sisteman fitxategien irakurketa arbitrarioa egin,
- administratzaile kontura sarbidea lortu eta Panorama-k administratutako gailuak manipulatu,
- shell komando arbitrarioak exekutatu root pribilegioekin,
- sistemaren prozesuak ustekabean itxi,
- administratzailearen ekintzak egin,
- kudeatutako suebakietara sarbide pribilegiatua lortu.

Ahultasun hauetarako honako identifikatzaileak esleitu dira: CVE-2020-2001, CVE-2020-2002, CVE-2020-2005, CVE-2020-2006, CVE-2020-2007, CVE-2020-2008, CVE-2020-2009, CVE-2020-2010, CVE-2020-2011, CVE-2020-2012, CVE-2020-2013, CVE-2020-2014, CVE-2020-2015, CVE-2020-2016, CVE-2020-2017 eta CVE-2020-2018.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun IBM i2 Analysts Notebook-en

Argitalpen data: 2020/05/14

Garrantzia: Altua

Kaltetutako baliabideak:

IBM i2 Analysts Notebook eta IBM i2 Analysts Notebook Premium, 9.2.1 bertsioa.

Azalpena:

Fortinet-en FortiGuard Labs-eko Honggang Ren eta Kexu Wang ikertzaileek larritasun altuko 15 ahultasunen berri eman dioten IBMri, memoriaren hondatze erakoak.

Konponbidea:

IBM i2 Analysts Notebook 9.2.1.1 eta IBM i2 Analysts Notebook Premium 9.2.1.1 bertsioetara eguneratzea, hurrenez hurren.

Xehetasuna:

- IBM i2 Intelligent Analysts Platform baliatuz erasotzaile lokal batek kode arbitrarioa exekuta lezake sisteman, memoriako akats batek eraginda. Erabiltzaile bat konbentzituz gero bereziki diseinatutako fitxategi bat ireki dezan, erasotzaileak ahultasun hori balia lezake sisteman kode arbitrarioa exekutatzeko. Ahultasun horretarako ondoko identifikatzaileak erreserbatu dira: CVE-2020-4261, CVE-2020-4262, CVE-2020-4266, CVE-2020-4265, CVE-2020-4257, CVE-2020-4264, CVE-2020-4258 eta CVE-2020-4263.
- IBM i2 Intelligent Analysts Platform baliatuz erasotzaile lokal batek kode arbitrarioa exekuta lezake sisteman, memoriako akats batek eraginda. Erabiltzaile bat konbentzituz gero bereziki diseinatutako fitxategi bat ireki dezan, erasotzaileak ahultasun hori balia

lezake sisteman kode arbitrarioa exekutatzeko erabiltzailearen pribilegioekin, edo aplikazioa blokea dadin eragin lezake. Ahultasun horretarako ondoko identifikatzaileak erreserbatu dira: CVE-2020-4468, CVE-2020-4343, CVE-2020-4422, CVE-2020-4285, CVE-2020-4288, CVE-2020-4467 eta CVE-2020-4287.

Etiketak: Eguneraketa, IBM, Ahultasuna

Mugez kanpoko irakurketa erako ahultasuna Exim-en

Argitalpen data: 2020/05/18

Garrantzia: Altua

Kaltetutako baliabideak:

Exim, 4.93 bertsioa eta lehenagokoak.

Azalpena:

DEVCOREko segurtasun ekipoko Orange Tsaik larritasun altuko ahultasun bat aurkitu du Exim-en SPA autentifikazio metodoan, mugez kanpoko irakurketa erakoa.

Konponbidea:

Exim-en 4.94 bertsiora eguneratzea.

Xehetasuna:

EExim4-k mugez kanpoko irakurketa erako ahultasun bat dauka SPAren autentifikazio kontrolatzailean. Horren ondorioz SPA/NTLM autentifikazioa saihets liteke auths/spa.c eta auths/auth-spa.c-n. Ahultasun horretarako CVE-2020-12783 identifikatzailea erabili da

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Osokoen gainezkatze erako ahultasuna PHP 7-n

Argitalpen data: 2020/05/18

Garrantzia: Altua

Kaltetutako baliabideak:

PHP7, 7.4.6 bertsioa baino lehenagokoak.

Azalpena:

PHPk osokoen gainezkatze erako kritikotasun altuko ahultasun bat aurkitu du.

Konponbidea:

PHP 7 eguneratzea 7.4.6 bertsiora.

Xehetasuna:

Fitxategi izen luzeak dituzten fitxategien igoerarekin lotuta dagoen *php-src/main/rfc1867.c*-ko akats bat baliatuz, osokoen gainezkatzea eragin liteke eta ondorioz blokeatzea gertatu. Ahultasun hori baliatuko lukeen urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake. Ahultasun horretarako CVE-2019-11048 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna, PHP

Zerbitzuaren ukapen erako ahultasuna IBM Spectrum Scale-n

Argitalpen data: 2020/05/19

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Spectrum Scale, honako bertsioak:

- 5.0.0.0 bertsiotik 5.0.4.3 bertsiora bitartean;
- 4.2.0.0 bertsiotik 4.2.3.21 bertsiora bitartean.

Azalpena:

Larritasun altuko ahultasun bat aurkitu da IBM Spectrum Scale-ren maila guztietan. Hori baliatuz erasotzaile lokal batek zerbitzuaren ukapena eragin lezake.

Konponbidea:

- IBM Spectrum Scale, 5.0.0.0 bertsiotik 5.0.4.3 bertsiora bitartean, 5.0.4.4 bertsiora eguneratzea;

- IBM Spectrum Scale, 4.2.0.0 bertsiotik 4.2.3.21 bertsiora bitartean, 4.2.3.22 bertsiora eguneratzea.

Xehetasuna:

IBM *Spectrum Scale*-ren fitxategien sistemaren osagaiak ahultasun bat dauka bere nukleoaren moduluan. Hori baliatuz erasotzaile batek zerbitzuaren ukapen egoera eragin lezake kaltetutako sisteman. Ahultasuna baliatzeko erasotzaile lokal batek *ioctls*-en (*input/output controls*) azpimultzo bat dei lezake *Spectrum Scale* gailuan baliagarriak ez diren argumentuekin, nukleoa blokeatzea eraginez. Ahultasun horretarako CVE-2020-4411 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Moodlen

Argitalpen data: 2020/05/19

Garrantzia: Altua

Kaltetutako baliabideak:

- 3.8 bertsiotik 3.8.2 bertsiora bitartekoak;
- 3.7 bertsiotik 3.7.5 bertsiora bitartekoak;
- 3.6 bertsiotik 3.6.9 bertsiora bitartekoak;
- 3.5 bertsiotik 3.5.11 bertsiora bitartekoak;
- zerbitzurik gabeko lehenagoko bertsioak.

Azalpena:

Paul Holden eta Abdullah Hussam ikertzaileek kritikotasun altuko bi ahultasunen berri eman dute, kodearen urruneko exekuzio eta gordetako Cross-Site Scripting (XSS) erakoak.

Konponbidea:

Moodlek hainbat eguneraketa argitaratu ditu, kaltetutako bertsioaren arabera:

- 3.8.3,
- 3.7.6,
- 3.6.10,
- 3.5.12.

Xehetasuna:

- MathJax-en 2.7.2 bertsioak eta lehenagokoek gordetako XSS erako ahultasun bat daukate. Ahultasun horretarako CVE-2018-1999024 kodea erabili da.
- Posible da SCORM pakete bat sortzea, eta hori ikastaro batera gehitzen denean kodearen urruneko exekuzioa egin liteke. Ahultasun horretarako CVE-2020-10738 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Ahultasunak ISCren BIND 9-n

Argitalpen data: 2020/05/20

Garrantzia: Altua

Kaltetutako baliabideak:

BINDen kaltetutako bertsioak:

- 9.0.0 bertsiotik 9.11.18 bertsiora bitartekoak;
- 9.12.0 bertsiotik 9.12.4-P2 bertsiora bitartekoak;
- 9.14.0 bertsiotik 9.14.11 bertsiora bitartekoak;
- 9.16.0 bertsiotik 9.16.2 bertsiora bitartekoak;
- 9.17.0tik garapen esperimentaleko 9.17 adarraren 9.17.1 bertsioraino;
- 9.13 eta 9.15 garapen adarretako bertsio zaharkitu guztiak;
- BIND Supported Preview Edition-en 9.9.3-S1etik 9.11.18-S1era bitarteko bertsio guztiak.

Azalpena:

Hainbat ikertzailek kritikotasun altuko bi ahultasunen berri eman diote ISCri.

Konponbidea:

BINDen honako bertsio hauetara eguneratzea:

- BIND 9.11.19,
- BIND 9.14.12,
- BIND 9.16.3,
- BIND Supported Preview Edition, BIND 9.11.19-S1 bertsiora eguneratzea.

Xehetasuna:

- Erantzun bat prozesatzen denean bilaketen kopuruan muga aski murriztailea ez dagoenez, urruneko erasotzaile batek sistemaren errendimenduan eragin lezake, edo anplifikazio eraso batean zerbitzaria erabili islatzaile modura. Ahultasun horretarako CVE-2020-8616 identifikatzailea erabili da.
- TSIG erregistroak dauzkaten mezuen baliozkotasuna egiaztatzen duen kodeak duen akats bat baliatuz, urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake. Ahultasun horretarako CVE-2020-8617 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak DNS, Ahultasuna

Kodearen injekzio erako ahultasuna VMware-ren Cloud Director-en

Argitalpen data: 2020/05/20

Garrantzia: Altua

Kaltetutako baliabideak:

vCloudDirector, honako bertsioak:

- 10.0.x, Linux eta PhotonOS appliancerako;
- 9.7.x, Linux eta PhotonOS appliancerako;
- 9.5.x, Linux eta PhotonOS appliancerako;
- 9.1.x, Linuxerako.

Azalpena:

Citadeloko bi ikertzailek kritikotasun altuko ahultasun baten berri eman diote VMwareri, kodearen injekzio erakoa.

Konponbidea:

vCloud Director-en kaltetutako bertsioak honako bertsioetara eguneratzea:

- 10.0.0.2,
- 9.7.0.5,
- 9.5.0.6,
- 9.1.0.4.

Xehetasuna:

VMware Cloud Director-ek ez ditu modu egokian erabiltzen sarrerak, eta ondorioz urruneko erasotzaile batek kodearen injekzioa egin lezake. Ahultasun horretarako CVE-2020-3956 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Hainbat ahultasun HPE produktuetan

Argitalpen data: 2020/05/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- HPE Superdome Flex Server, 3.25.46 baino lehenagoko bertsioak;
- Nimble Storage Hybrid Flash Arrays, Nimble Storage All Flash Arrays eta Nimble Storage Secondary Flash Arrays, 3.9.2.0, 4.5.5.0, 5.0.8.0, 5.1.4.0 eta lehenagoko bertsioak.

Azalpena:

HPEk Superdome Flex Server eta HPE NimbleOS-ek dituzten hiru ahultasun argitaratu ditu, 2 kritikoak eta bat altua. Horiek baliatuz erasotzaile batek pribilegioen eskalatzea egin lezake, edo informazio sentikorrera edo sistemakora sarbidea lortu eta hura aldatu.

Konponbidea:

- HPE Superdome Flex Server, 3.25.46 bertsiora edo berriago batera eguneratzea;
- HPE NimbleOS, 3.9.3.0, 4.5.6.0, 5.0.9.0, 5.1.4.100 edo geroagoko bertsioetara eguneratzea.

Xehetasuna:

- HPE Superdome Flex Server-en osagai batek duen baliozkotze akats bat dela eta, erasotzaile lokal batek pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2020-7137 identifikatzailea erabili da.
- HPE Nimble Storage sistemek duten kodearen urruneko exekuzio erako ahultasunak baliatuz, erasotzaile batek pribilegioen eskalatzea egin lezake bektorean. Ahultasun horretarako CVE-2020-7138 identifikatzailea erabili da.
- HPE Nimble Storage sistemek duten urruneko sarbide erako ahultasunak baliatuz, erasotzaile batek informazio sentikorrera edo sistemakora sarbidea lor lezake eta hura aldatu. Ahultasun horretarako CVE-2020-7139 identifikatzailea erabili da.

Etiketak: Eguneraketa, HP, Ahultasuna

Hainbat ahultasun TIBCOren JasperReports-en

Argitalpen data: 2020/05/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- TIBCO JasperReports Server, honako bertsioak:
  - 7.5.0;
  - 7.2.0;
  - 7.1.1 eta lehenagokoak;
- AWS Marketplace-rako TIBCO JasperReports Server, 7.5.0 eta lehenagoko bertsioak;

- ActiveMatrix BPMrako TIBCO JasperReports Server, 7.1.1 eta lehenagoko bertsioak;
- TIBCO JasperReports Library, honako bertsioak:
  - 7.5.0;
  - 7.3.0;
  - 7.2.1;
  - 7.2.0;
  - 7.1.1 eta lehenagokoa;
- ActiveMatrix BPMrako TIBCO JasperReports Library, 7.1.1 eta lehenagoko bertsioak;
- administrative UI eta report generator osagaiak.

Azalpena:

Bi ahultasun aurkitu dira, bat larritasun kritikokoa eta bestea altukoa, pribilegioen eskalatze eta HTML injekzio erakoak.

Konponbidea:

- TIBCO JasperReports Server:
  - 7.1.1 eta lehenagoko bertsioen kasuan, 7.1.3 edo bertsio berriagoetara eguneratzea;
  - 7.2.0 eta lehenagoko bertsioen kasuan, 7.2.1 edo bertsio berriagoetara eguneratzea;
  - 7.5.0 eta lehenagoko bertsioen kasuan, 7.5.1 edo bertsio berriagoetara eguneratzea;
- AWS Marketplace-rako TIBCO JasperReports Server, 7.5.0 eta lehenagoko bertsioen kasuan,7.5.1 edo bertsio berriagoetara eguneratzea;
- ActiveMatrix BPMrako TIBCO JasperReports Server, 7.1.1 eta lehenagoko bertsioen kasuan,7.1.3 edo bertsio berriagoetara eguneratzea;
- TIBCO JasperReports Library:
  - 7.1.1 eta lehenagoko bertsioen kasuan, 7.1.3 edo bertsio berriagoetara eguneratzea;
  - 7.2.0 eta 7.2.1 bertsioen kasuan, 7.2.2 edo geroagoko bertsioetara eguneratzea;
  - 7.3.0 bertsioaren kasuan, 7.3.1 edo bertsio berriagoetara eguneratzea;
  - 7.5.0 bertsioaren kasuan, 7.5.1 edo bertsio berriagoetara eguneratzea;
- ActiveMatrix BPMrako TIBCO JasperReportsLibrary, 7.1.1 eta lehenagoko bertsioen kasuan,7.1.3 edo bertsio berriagoetara eguneratzea.

Xehetasuna:

- Autentifikatu gabeko urruneko erasotzaile batek superuser baimenak eskura litzake JasperReports Server-en eta kaltetutako sisteman kode arbitrarioa exekutatu. Ahultasun horretarako CVE-2020-9409 identifikatzailea erreserbatu da.
- Erasotzaile batek HTML injekzio bat egin lezake (XSS iraunkor modura ere ezaguna) txostenak sortzeko osagaiaren irteera duen web interfaze baten kontrol osoa eskuratzeko. Horrela, bereziki diseinatutako txosten bat ikusten duen pribilegiorik altueneko jabearen pribilegio maila eskuratu ahal izango luke. Ahultasun horretarako CVE-2020-9410 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Ciscoren produktuetan

Argitalpen data: 2020/05/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco Unified Contact Center Express (CCX), 12.0 eta lehenagoko bertsioak;
- Cisco Prime Network Registrar, 8.3, 9.0, 9.1, 10.0 eta 10.1 bertsioak.

Azalpena:

Booz Allen Hamilton-eko Brenden Meeder-ek eta Cisco Technical Assistance Center-ek (TAC) larritasun kritiko eta altuko bi ahultasunen berri eman dute, biak sarreraren baliozkotze oker erakoak.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak, ohartarazpen bakoitzeko *Fixed Releases* atalean zehaztuak, Software Ciscoren deskarga panelean eskura daitezke.

Xehetasuna:

Ahultasun horiek baliatuko lituzkeen autentifikatu gabeko urruneko erasotzaile batek honako ekintzak egin litzake:

- kodearen urruneko exekuzioa,
- zerbitzuaren ukapena (DoS).

Honako identifikatzaile hauek erreserbatu dira: CVE-2020-3280 eta CVE-2020-3272.

Etiquetas: Eguneraketa, Cisco, Ahultasuna

Zerbitzuaren ukapen erako ahultasuna Microsoften Windows DNS Server-en

Argitalpena data: 2020/05/21

Garrantzia: Altua

Kaltetutako baliabideak:

Todas las versiones de Windows DNS Server.

Azalpena:

Tel-Aviveko Unibertsitateko Yehuda Afek eta Lior Shafir ikertzaileek, eta IDC Herzliya-ko Anat Bremler-Barr-ek Microsofti ahultasun baten berri eman diote, Windowsen DNS zerbitzariei eragiten diena. Erasotzaile batek ahultasun hori balia lezake zerbitzuaren ukapen egoera eragiteko.

Konponbidea:

DNSren anplifikazio arazoaren arintze neurri modura, biktima Microsoften DNSa zerbitzaria erabiltzen ari bada, Response Rate Limit (RRL) funtzionaltasuna gaitzea gomendatzen da.

Xehetasuna:

Erasotzaile batek Windowsen DNS zerbitzariei eragiten dien paketeen anplifikazioarekin zerikusia duen ahultasun hau balia lezake hedatutako zerbitzuaren ukapen egoera (DDoS) eragiteko, eta horrela DNS zerbitzariaren zerbitzuak ez erantzutea lortuko luke.

Etiketak: DNS, Microsoft, Ahultasuna, Windows

Kodearen urruneko exekuzioaren erako ahultasuna Apache Tomcat-en

Argitalpen data: 2020/05/21

Garrantzia: Altua

Kaltetutako baliabideak:

Apache Tomcat, honako bertsioak:

- 7.0.0 bertsiotik 7.0.103 bertsiora bitartekoak;
- 8.5.0 bertsiotik 8.5.54 bertsiora bitartekoak;
- 9.0.0.M1 bertsiotik 9.0.34 bertsiora bitartekoak;
- 10.0.0-M1 bertsiotik 10.0.0-M4 bertsiora bitartekoak.

Azalpena:

pdd security research-eko Jarvis Threedr3am ikertzaileak Apache Tomcat-eko segurtasun ekipoari kritikotasun altuko ahultasun baten berri eman dio, kodearen urruneko exekuzio erakoa.

Konponbidea:

Apache Tomcat honako bertsio hauetara eguneratzea:

- 7.0.104,
- 8.5.55,
- 9.0.35,
- 10.0.0-M5.

Xehetasuna:

Bereziki sortutako erantzun bat bidaltzen duen urruneko erasotzaile batek kodearen urruneko exekuzioa egin lezake bere kontrolpeko fitxategiaren deserializazioaren bidez. Ahultasun horretarako CVE-2020-9484 identifikatzailea erabili da.

Etiketak: Eguneraketa, Apache, Ahultasuna

Ahultasuna Drupal-en core-an

Argitalpen data: 2020/05/21

Garrantzia: Ertaina

Kaltetutako baliabideak:

Honako bertsioak:

- 8.8.6;
- 8.7.14;
- 7.70.

Azalpena:

jQuery-k dituen bi segurtasun ahultasun argitaratu dira, Drupal-en bertsio batzuei eragiten dietenak. Era berean, Drupal 7-k duen birbideratze ireki erako beste ahultasun baten berri eman da.

Konponbidea:

8.8.6, 8.7.14 o 7.70 bertsioetara eguneratzea.

Xehetasuna:

- jQuery-k dituen XXL erako bi ahultasunak baliatuz, erasotzaile batek fidagarria ez den kodea exekuta lezake, fidagarriak ez diren jatorrietako HTML bat jQuery-ren DOM manipulazio metodoetako batera (hau da, .html(), .append(), eta beste batzuk) pasatzean, baita hura saneatu ondoren ere. Ahultasun horietarako CVE-2020-11022 eta CVE-2020-11023 identifikatzaileak erabili dira.
- drupal_goto() funtzioan xede den kontsultaren parametroaren baliozkotze ez-nahiko baten ondorioz, Drupal 7-k duen birbideratze ireki erako ahultasun bat baliatuz, erasotzaile batek erabiltzaileak engaina litzake bereziki diseinatutako lotura bat bisita dezaten, kanpoko URL arbitrario batera birbideratuko dituena.

Etiketak: Eguneraketa, CMS, Ahultasuna

SQL injekzio arloko ahultasuna GESIO sisteman

Argitalpen data: 2020/05/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

GESIO ERP, 11.2 bertsioaren aurrekoak.

Azalpena:

INCIBE erakundeak ahultasun baten berri eman du GESIO ERP softwarean, INCIBE-2020-225 barne kodearekin. Francisco Palmak, Luis Vázquezek eta Diego Leónek aurkitu zuten.

CVE-2020-8967 kodea esleitu zaio ahultasun horri. 10eko oinarri puntuazioa kalkulatu da, CVSS v3 kodearen arabera; CVSS kalkulua honakoa da: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H.

Konponbidea:

11.2 bertsiora eguneratzea.

Xehetasuna:

GESIO ERP sistema SQL INJEKZIOAREN eraginpean dago, cms_plantilla_sites.php artxiboko "idsite" URL parametroan.

Ahultasun horren bidez, urrutiko erasotzaile batek honako hiru ekintzak gauzatu litzake, gutxienez:

- Akatsean oinarritutako erasoa,
- Denboran oinarritutako erasoa,
- Batasunagatiko erasoa.

Ahultasun horren ondorioz, erasotzaile bat gai izango litzateke datu-basearen informazio osoa berreskuratzeko.

GESIO sistemak honako ekintzak zabaldu ditu arazoa konpontzeko:

- Barne-prozedurak hobetzea.
- Fronted-ean injekzioaren aurkako programazio kontrol berriak ezartzea. 11.2 bertsiotik aurrera egongo dira eskuragarri.
- Backend funtzioetan hobekuntza osagarriak egitea, 11.2 bertsiotik aurrera ere eskuragarri egongo direnak.

CWE-89: SQL komando batean erabilitako komando berezien neutralizazio okerra (SQL injekzioa).

Denbora lerroal:

2019/04/02 ? Ikertzaileen ikerketa.

2020/04/08 ? Ikertzaileak INCIBErekin jarri dira harremanetan.

2020/04/21 ? GESIOren segurtasun-taldeak INCIBEri baieztatu dio ahultasuna, zuzenketa bertsioa eta softwarearen partxea v11.2an argitaratu direla adieraziz (Segurtasun-partxea).

2020/06/01 ? Abisua INCIBE erakundeak argitaratu du.

Abisu horren inguruko informazio gehiago baduzu, jar zaitez harremanetan INCIBErekin, CNAren ahultasun-erreportean adierazten den moduan.

Etiketak: 0day, Ahultasuna, CNA, Eguneratzea

Hainbat ahultasun VMwareren produktuetan

Argitalpen data: 2020/05/29

Garrantzia: Altua

Katetutako baliabideak:

- VMware ESXi, 6.7 eta 6.5 bertsioak;
- VMware Workstation Pro / Player (Workstation), 15.X bertsioa;
- VMware Fusion Pro / Fusion (Fusion), 11.X bertsioa;
- Mac-erako VMware Remote Console (Mac-erako VMRC), 11.X eta lehenagoko bertsioak;
- Mac-erako VMware Horizon Client, 5.X eta lehenagoko bertsioak.

Azalpena:

Zibersegurtasuneko hainbat ikertzailek VMware-ri kritikotasun altu, ertain eta baxuko hiru ahultasunen berri eman diote, pribilegioen eskalatze, sarbidearen kontrol desegoki eta sistemaren ustekabeko itxiera erakoak.

Konponbidea:

VWwarek hainbat eguneraketa argitaratu ditu, kaltetutako produktu eta bertsioen arabera. Eguneraketa zehatza eskuratzeko *Erreferentziak* atala kontsultatu.

Xehetasuna:

- Kritikotasun altuko ahultasunak VMware Fusion, Mac-erako VMRC eta Mac-erako Horizon Client produktuei eragiten die. Produktu horiek pribilegioen eskalatze lokal erako ahultasun bat daukate, service opener-en Time-of-check Time-of-use-k (TOCTOU) duen

akats baten ondorioz. Pribilegio normalak dituen erasotzaile batek pribilegioen eskalatzea egin lezake eta sisteman root pribilegioak eskuratu. Ahultasun horretarako CVE-2020-3957 identifikatzailea erreserbatu da.
- Kritikotasun ertain eta baxuko ahultasunetarako CVE-2020-3958 eta CVE-2020-3959 identifikatzaileak erreserbatu dira, hurrenez hurren.

Etiketak: Eguneraketa, VMware, Ahultasuna

Ahultasunak IBMren Security Identity Governance and Intelligence-n (IGI)

Argitalpen data: 2020/05/29

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Security Identity Governance and Intelligence, 5.2.6 bertsioa.

Azalpena:

IBMk Security Identity Governance and Intelligence (IGI) bere produktuak dituen barneratutako pasahitzen ahultasun bat eta XML External Entity Injection (XEE) injekzio erako beste bat argitaratu ditu.

Konponbidea:

5.2.6.0-ISS-SIGI-FP0001 bertsiora eguneratzea.

Xehetasuna:

- IBM Security Identity Governance and Intelligencek (IGI) erabiltzen duen IBM Security Directory Integrator-en bertsioan dauden barneratutako pasahitzak ezabatu ditu IBMk.
- Virtual Appliancek XML External Entity Injection (XXE) erako eraso bat jasan lezake. Hori baliatuz urruneko erasotzaile batek informazio sentikorra agerian utz lezake, edo memoriako baliabideak kontsumitu. Ahultasun horretarako CVE-2020-4246 identifikatzailea erabili da.

Etiketak: Eguneraketa, IBM, Ahultasuna