2019ko Uztailaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun IBMren produktuetan

Argitalpen data: 2019/07/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IBM Spectrum Protect Plus, 10.1.3 bertsioa eta lehenagokoak;
- IBM Spectrum Protect eta Storage Agents:
  - 8.1.0.0 bertsiotik 8.1.7.xxx bertsiora bitartekoak;
  - 7.1.0.0 bertsiotik 7.1.9.200 bertsiora bitartekoak;
- IBM Cognos TM1, 10.2.2 bertsioa.

Azalpena:

IBMk hainbat ahultasun aurkitu ditu, horietatik bat larritasun kritikokoa, lau altukoak eta bat ertainekoa.

Konponbidea:

- IBM Spectrum Protect Plus, 10.1.4 bertsiora eguneratzea;
- IBM Spectrum Protect eta Storage Agents:
  - 8.1 adarraren kasuan, 8.1.8 bertsiora eguneratzea;
  - 7.1 adarraren kasuan, 7.1.9.300 bertsiora eguneratzea;
- IBM Cognos TM1 10.2.2ren kasuan, Cognos TM1 10.2.2.7 Interim Fix 22 segurtasun partxea aplikatzea.

Xehetasuna:

- IBM Spectrum Protect eta Storage Agents-ek duten larritasun kritikoaren jatorria da pilan oinarritutako bufferraren gainezkatzea. Urruneko erasotzaile batek instantziako identitate pribilegioekin kode arbitrarioa exekuta lezake edo sistema gelditu. Ahultasun horretarako CVE-2019-4087 identifikatzailea erreserbatu da.
- IBM Spectrum Protect eta Storage Agents-ek duten kritikotasun altuko ahultasun baten jatorria da dsmqsan moduluan bereziki sortutako liburutegi bat kargatzea. Erasotzaile lokal batek root pribilegioak eskura litzake sisteman. Ahultasun horretarako CVE-2019-4088 identifikatzailea erreserbatu da.
- IBM Cognos TM1ek duen kritikotasun altuko ahultasun baten jatorria da CreateProcess() eta CreateProcessAsUser() funtzioek egiten dituzten dei ez-seguruak Windowsen bilaketen bideak erabiltzean kakotxen artean jarri gabe. Erasotzaile lokal batek kode arbitrarioa exekuta lezake pribilegioen eskalatzearekin. Ahultasun horretarako CVE-2019-4245 identifikatzailea erreserbatu da.
- IBM Spectrum Protect Plus-ek duen kritikotasun altuko ahultasun baten jatorria da berau erabiltzea Oracle edo MongoDB datu baseak babesteko. Erasotzaile batek pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2019-4383 identifikatzailea erreserbatu da.
- IBM Spectrum Protect Plus-ek duen kritikotasun altuko ahultasun baten jatorria da berau erabiltzea Oracle, DB2 edo MongoDB datu baseak babesteko. Erasotzaile batek kode arbitrarioa exekuta lezake sisteman. Ahultasun horretarako CVE-2019-4357 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Ziurtagirien uholdea OpenPGPn

Argitalpen data: 2019/07/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- OpenPGP ziurtagiriak SKS gakoen zerbitzariaren sarean ostatatuta.

Azalpena:

Robert J. Hansen eta Daniel Kahn Gillmor-ek OpenPGPk dituen hainbat ahultasunen berri eman dute. Horien jatorria da SKS gakoen zerbitzariek "soilik idazketa"-ren diseinuan duten akatsa, zerbitzuaren ukapen egoera eragin lezakeena.

Konponbidea:

- OpenPGP ziurtagiriak eguneratzeko SKS gakoen zerbitzarien sarea ez erabiltzea. Horren ordez, ordezko zerbitzari bat erabiltzea, keys.openpgp.org esate baterako.
- Pozoitutako ziurtagiri publikoak giltzatakotik ezabatzea, eta berriz eskuratzea bide fidagarri batetik.

Xehetasuna:

SKS ahula da ziurtagirien uholde erako erasoen aurrean, soilik idazketakoa den bere diseinuaren ondorioz. Hori baliatuz erasotzaile batek OpenPGP ziurtagiriak pozoitu litzake, ezabatu ezin daitezkeen "spam" sinadura kopuru handi bat gehituz. Pozoiduraren ondorioz GnuPGk ezin ditu inportatu ziurtagiriak SKS gakoen zerbitzarietatik, eta horren eraginez zerbitzuaren ukapen egoera gertatzen da.

Etiketak: Ahultasuna

Hainbat ahultasun Dell EMCren iDRACen

Argitalpen data: 2019/07/02

Garrantzia: Handia

Kaltetutako baliabideak:

- Dell EMC iDRAC6, 2.92 baino lehenagoko bertsioak;
- Dell EMC iDRAC7/iDRAC8, 2.61.60.60 baino lehenagoko bertsioak;
- Dell EMC iDRAC9, ondoren aipatutakoak baino lehenagoko bertsioak;
  - 3.21.24.22;
  - 3.21.25.22;
  - 3.21.26.22;
  - 3.22.22.22;
  - 3.23.23.23;
  - 3.24.24.24;
  - 3.30.30.30.

Azalpena:

Dell EMCk kritikotasun altuko hiru ahultasun aurkitu ditu iDRAC familiako hainbat produktutan. Urruneko erasotzaile batek kode arbitrarioa exekuta lezake, autentifikazioa saihestu edo sistema blokeatu.

Konponbidea:

- iDRAC9ren firmwarea honako bertsioetara eguneratzea:
  - 3.20.21.20;
  - 3.21.24.22;
  - 3.21.25.22;
  - 3.21.26.22;
  - 3.22.22.22;
  - 3.23.23.23;
  - 3.24.24.24;
  - 3.30.30.30.
- iDRAC8 eta iDRAC7ren firmwarea 2.61.60.60 bertsiora eguneratzea.
- iDRAC6ren firmwarea 2.92 bertsiora eguneratzea.

Xehetasuna:

- Ahultasun baten jatorria pilan oinarritutako bufferraren gainezkatzea da. Urruneko erasotzaile batek webserver pribilegioekin kode arbitrarioa exekuta lezake edo sistema gelditu. Ahultasun horretarako CVE-2019-3705 identifikatzailea erabili da.
- Ahultasun baten jatorria da bereziki sortutako datuen bidalketa iDRACen web interfazera. Urruneko erasotzaile batek autentifikazioaren saihestea egin lezake sisteman. Ahultasun horretarako CVE-2019-3706 identifikatzailea erabili da.
- Ahultasun baten jatorria da bereziki sortutako sarrera datuen bidalketa WS-MANen interfazera. Urruneko erasotzaile batek autentifikazioaren saihestea egin lezake sisteman. Ahultasun horretarako CVE-2019-3707 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun F5en produktuetan

Argitalpen data: 2019/07/02

Garrantzia: Handia

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), honako bertsioak:
  - 14.0.0 - 14.1.0.5;
  - 13.0.0 - 13.1.1.4;
  - 12.1.0 - 12.1.4;
  - 11.5.1 - 11.6.4.
- F5 SSL Orchestrator, ondoko bertsioak:
  - 14.0.0;
  - 14.1.0.

Azalpena:

F5ek hainbat eratako ahultasunen berri eman du: XSS, DoS, komandoen injekzioa eta ezagutarazi gabeko trafikoaren fluxua.

Konponbidea:

Honako bertsioetara eguneratzea:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator):
  - 15.0.0;
  - 14.1.0.6;
  - 13.1.1.5;
  - 12.1.4.1;
  - 11.6.4;
  - 11.5.9.
- F5 SSL Orchestrator:
  - 15.0.0;
  - 14.1.0.6.

Xehetasuna:

- Islatutako cross-site scripting (XSS) erako ahultasunak daude konfigurazio utilitate modura ere ezaguna den Traffic Management User Interface-ren (TMUI) ezagutarazi gabeko orrialde batean. Hori baliatuz erasotzaile batek komandoak exekuta litzake administratzaile pribilegioekin. Ahultasun horietarako CVE-2019-6625 eta CVE-2019-6626 identifikatzaileak erreserbatu dira.
- Urruneko erasotzaile batek zerbitzua eten lezake, Traffic Management Microkernel-en (TMM) berrabiatzea eraginez. Arazo horrek soilik eragiten die SNAT gaituta dutenean proxy-ren kateatze garden bat egiten duten F5 SSL Orchestrator sistemei. Ahultasun horretarako CVE-2019-6627 eta CVE-2019-6630 identifikatzaileak erreserbatu dira.
- Ezagutarazi gabeko iControl REST worker ahula da administratzaile pribilegioak dituen erabiltzaile batek komandoak injektatzen dituenean. Arazo honek eragiten die bai iControl RESTen eta bai tmsh-en inplementazioei. Ahultasun horretarako CVE-2019-6620, CVE-2019-6621 eta CVE-2019-6622 identifikatzaileak erreserbatu dira.
- BIG-IP iSession zerbitzari birtualera bidaltzen den ezagutarazi gabeko trafikoak eragin dezake Traffic Management Microkernel (TMM) berrabiatzea, zerbitzuaren ukapen egoera (DoS) sortuz. Ahultasun horretarako CVE-2019-6623 identifikatzailea erreserbatu da.
- Urruneko erasotzaile batek Traffic Management Microkernel (TMM) berrabiatzea eragin dezake, sistema ahulean zerbitzuaren ukapen egoera (DoS) sortuz. Ahultasun horretarako CVE-2019-6624 identifikatzailea erreserbatu da.
- Eskuragarritasun alturako (HA) konfiguratutako BIG-IP PEM sistema batean eta baldintza batzuetan, TMM prozesua amai daiteke eta berrabiarazi, BIG-IP PEM trafikoa OpenVPN classifier-ekin prozesatzen den bitartean. Ahultasun horretarako CVE-2019-6628 identifikatzailea erreserbatu da.
- Trafikoaren prozesamendua eten egiten da Traffic Management Microkernel (TMM) berrabiatzen den bitartean. Kaltetutako F5 gailua gailuen talde bateko zati bezala konfiguratzen denean, akats batengatik sistemak kommutazio bat aktibatuko du gailu parekidean. Ahultasun horretarako CVE-2019-6629 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/07/04

Garrantzia: Handia

Kaltetutako baliabideak:

- Cisco Web Security Appliance-rako (WSA) Cisco AsyncOS Software, bai gailu birtualetarako eta bai hardwarerako, gailuek HTTPS proxy funtzioa gaituta dutenean eta gutxienez deszifratze politika bat konfiguratuta dutenean.
- Cisco Small Business 200, 300, eta 500 Series Managed Switches, 1.4.10.6 baino lehenagoko software bertsioak exekutatzen dituztenak, HTTPS baimentzeko administrazioaren web interfazea gaituta edo konfiguratuta dagoenean.
- Cisco Enterprise NFV Infrastructure Software (NFVIS), 3.10.1 baino lehenagoko bertsioak.
- Cisco Nexus 9000 Series Fabric Switches, ACI moduan, 14.1(2g) baino lehenagoko software bertsioa exekutatzen dutenean eta fabrikatik lehenetsita datorren modu permisiboaren konfigurazioa erabiltzen dutenean.
- Windowserako Cisco Jabber, 12.6(0) baino lehenagoko bertsioak.
- Cisco Unified Communications Manager.
- Cisco APIC Software, 4.1(2g) baino lehenagoko bertsioak.

Azalpena:

Ciscok kritikotasun altuko hamar ahultasunen berri eman du. Erasotzaile batek hainbat eratako erasoak egin litzake: zerbitzuaren ukapena (DoS), memoria hondatzea, fitxategi arbitrarioen irakurketa edo idazketa, komandoen injekzioa, baimenik gabeko sarbidea, DLLren aurrekarga eta pribilegioen eskalatzea.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Ciscoren softwarearen deskarga paneletik deskarga daitezke.

Xehetasuna:

Ahultasunen jatorriak honakoak dira:

- Secure Sockets Layer (SSL) zerbitzari ziurtagirien baliozkotze ez-nahikoa HTTPS deszifratze funtzioan. Autentifikatu gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake. Ahultasun horretarako CVE-2019-1886 identifikatzailea erreserbatu da.
- Baliozkotze okerra HTTPS paketeen sarrera prozesatzailean. Autentifikatu gabeko urruneko erasotzaile batek memoriaren hondatzea eragin lezake kaltetutako gailu batean. Ahultasun horretarako CVE-2019-1892 identifikatzailea erreserbatu da.
- Web interfazera bidalitako eskarien baliozkotze okerra. Autentifikatu gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake. Ahultasun horretarako CVE-2019-1891 identifikatzailea erreserbatu da.
- NFVIS fitxategien sistemako komandoetan sarreraren baliozkotze okerra. Autentifikatutako eta administratzaile pribilegioak lituzkeen urruneko erasotzaile batek azpiko sistema eragilean fitxategi arbitrarioak gainidatz edo irakur litzake. Ahultasun horretarako CVE-2019-1894 identifikatzailea erreserbatu da.
- shell-aren erabiltzaile lokal batentzat eskuragarria den konfigurazio fitxategi baten sarreraren baliozkotze ez-nahikoa. root modura autentifikatutako erasotzaile lokal batek komando arbitrarioak exekuta litzake sistema eragilean. Ahultasun horretarako CVE-2019-1893 identifikatzailea erreserbatu da.
- Segurtasun baldintza ez-nahikoak VLAN azpiegiturako Link Layer Discovery Protocol-en (LLDP) konfigurazio fasean. Autentifikatu gabeko alboko erasotzaile batek segurtasun baliozkotzeak saihets litzake eta baimendu gabeko zerbitzari bat konekta lezake azpiegiturako VLANera. Ahultasun horretarako CVE-2019-1890 identifikatzailea erreserbatu da.

- Aplikazioak exekuzio denboran kargatutako baliabideen baliozkotze ez-nahikoa. Autentifikatutako erasotzaile lokal batek DLLren aurrekarga eraso bat egin lezake. Ahultasun horretarako CVE-2019-1855 identifikatzailea erreserbatu da.
- Sarrerako SIP trafikoaren baliozkotze ez-nahikoa. Autentifikatu gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake. Ahultasun horretarako CVE-2019-1887 identifikatzailea erreserbatu da.
- Fitxategi bidearen baliozkotze eta akatsen egiaztatze osagabeak software jakin bat kargatzen denean. Autentifikatutako urruneko erasotzaile batek pribilegioak eskala litzake eta root baimenak eskuratu kaltetutako gailu batean. Ahultasun horretarako CVE-2019-1889 identifikatzailea erreserbatu da.
- Kaltetutako gailu baten bidez bidalitako HTTP/HTTPS eskaeren eremu batzuen kasuan sarreraren baliozkotze mekanismo ez-nahikoak. Autentifikatutako urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake kaltetutako gailuan. Ahultasun horretarako CVE-2019-1884 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Ahultasuna HPEren UIoT-en

Argitalpen data: 2019/07/08

Garrantzia: Handia

Kaltetutako baliabideak:

- HPE Universal Internet of Things (UIoT), honako bertsioak:
  - 1.6;
  - 1.5;
  - 1.4.2;
  - 1.4.1;
  - 1.4.0;
  - 1.2.4.2.

Azalpena:

HPEk kritikotasun altuko ahultasun bat aurkitu du UIoTen hainbat bertsiotan.

Konponbidea:

- UIoT 1.6 bertsioen kasuan, 1.6 RP603 bertsiora eguneratzea.
- UIoT 1.5 bertsioen kasuan, 1.5 RP503 HF3 bertsiora eguneratzea.
- UIoT 1.5 baino lehenagoko bertsioen kasuan, esate baterako UIoT 1.4.0, 1.4.1, 1.4.2 eta 1.2.4.2, 1.5 RP503 HF3 edo 1.6 RP603 bertsioetara eguneratzea.

Xehetasuna:

UIoTek duen ahultasuna baliatuz urruneko erasotzaile batek baimenik gabeko sarbidea lor lezake gailura edo informazio sentikorrera. Ahultasun horretarako CVE-2019-11990 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, HP, IoT, Ahultasuna

Ahultasuna HPEren 3PAR Service Processor-en

Argitalpen data: 2019/07/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HPE 3PAR Service Processor (SP), 4.1etik 4.4ra bitarteko bertsioak.

Azalpena:

HPEk larritasun kritikoko ahultasun bat aurkitu du 3PAR Service Processor-en hainbat bertsiotan. Hori baliatuz konfidentzialtasuna, integritatea eta eskuragarritasuna eten litezke.

Konponbidea:

- HPE 3PAR Service Processor-en 4.4 MU9 (SP-4.4.0.GA-142) bertsiora eguneratzea.
- 3PARen sistema eragilearen uneko bertsioa 3.2.2EMU4 edo 3.2.2MU6 ez bada, 3PARen eguneraketarako laguntza ingurunea kontsultatu Service Processor eta HPE 3PARen sistema eragilea eguneratzeko.

Xehetasuna:

HPE 3PAR Service Processor-ek informazioa urrunetik zabaldu ahal izatearen ahultasuna dauka. Hori baliatuz erasotzaile batek Service Processor-en eta administratutako beste edozein 3PAR array-ren konfidentzialtasuna, integritatea eta eskuragarritasuna eten litzake. Ahultasun horretarako CVE-2019-11991 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, HP, Ahultasuna

2019ko uztaileko Microsoften segurtasun buletina

Argitalpen data: 2019/07/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows,
- Internet Explorer,
- Microsoft Edge,
- Microsoft Office and Microsoft Office Services and Web Apps,
- Azure DevOps,
- Open Source Software,
- .NET Framework,
- Azure,
- SQL Server,
- ASP.NET,
- Visual Studio,
- Microsoft Exchange Server.

Azalpena:

Segurtasun eguneraketei buruzko Microsoften uztaileko argitalpenean 75 ahultasun jaso dira, 15 kritiko gisa sailkatu dira eta 60 garrantzitsu gisa.

Konponbidea:

Dagozkien segurtasun eguneraketak instalatzea. Eguneraketen beraien instalazioari buruzko informazio orrian hori egiteko metodo ezberdinei buruzko argibideak daude.

Xehetasuna:

Argitaratutako ahultasun motak honako hauek dira:

- Kodearen urruneko exekuzioa,Informazioaren zabalkundea,
- Pribilegioen igoera,
- Zerbitzuaren ukapena,
- Segurtasunari ihes egitea,
- Ordezpena.

Etiketak: Eguneraketa, Microsoft, Ahultasuna

Ahultasuna Intel® Processor Diagnostic Tool-en

Argitalpen data: 2019/07/10

Garrantzia: Handia

Kaltetutako baliabideak:

- Intel® Processor Diagnostic Tool for 32-bit, 4.1.2.24_32bit baino lehenagoko bertsioak.
- Intel® Processor Diagnostic Tool for 64-bit, 4.1.2.24_64bit baino lehenagoko bertsioak.

Azalpena:

Intel® Processor Diagnostic Tool-ek duen ahultasun baten berri argitaratu da. Hori baliatuz erasotzaile batek pribilegioak eskala litzake, zerbitzuaren ukapen egoera eragin edo informazioa zabaldu.

Konponbidea:

Intel® Processor Diagnostic Tool 4.1.2.24 edo geroagoko bertsio batera eguneratzea.

Xehetasuna:

4.1.2.24 bertsioa baino lehenagoko Intel® prozesatzailearen diagnostiko tresnak duen sarbidearen kontrol desegoki erako ahultasun bat baliatuz, autentifikatutako erabiltzaile batek pribilegioen eskalatzea, informazioa hedatzea edo zerbitzuaren ukapena eragin litzake sarbide lokalaren bidez. Ahultasun horretarako CVE-2019-11133 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

SAPen segurtasun eguneraketa 2019ko uztailean

Argitalpen data: 2019/07/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Diagnostic Agent (LM-Service), 7.20 bertsioa.SAP NetWeaver Process Integration ABAP-en testak (SAP Basis), 7.0, 7.1, 7.3, 7.31, 7.4 eta 7.5 bertsioak.
- SAP Commerce Cloud (lehen SAP Hybris Commerce) (HY_COM), 6.3, 6.4, 6.5, 6.6, 6.7, 1808 eta 1811 bertsioak.
- OpenUI5, lehenagoko bertsioak eta ondoko hauek barne: 1.38.39, 1.44.39, 1.52.25, 1.60.6 eta 1.63.0.
- SAP Information Steward, 4.2 bertsioa.
- ABAP Server eta ABAP Platform (SAP Basis), 7.31, 7.4 eta 7.5 bertsioak.
- SAP BusinessObjects Business Intelligence Platform (BI Workspace) (Enterprise), 4.1, 4.2 eta 4.3 bertsioak.
- SAP NetWeaver for Java Application Server (Web Container), honako bertsioak: engineapi (7.1, 7.2, 7.3, 7.31, 7.4 eta 7.5) eta servercode (7.2, 7.3, 7.31, 7.4 eta 7.5).
- SAP ERP HCM (SAP_HRCES), 3 bertsioa.
- SAP NetWeaver Application Server for Java (Startup Framework), 7.21, 7.22, 7.45, 7.49, eta 7.53 bertsioak.
- SAP Gateway, 7.5, 7.51, 7.52 eta 7.53 bertsioak.

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 11 segurtasun ohar argitaratu ditu. Horietatik 1 larritasun kritikokoa da, 1 larritasun altukoa eta beste 9 larritasun ertainekoak.

Argitaratutako ahultasun motak honako hauek dira:

- *Cross-Site Scripting* (XSS) erako 4 ahultasun.Kode injekzioko ahultasun bat.
- Sistema eragileko komandoen injekzio erako ahultasun bat.
- Zerbitzuaren ukazioko ahultasun bat.
- Informazioaren zabalkundeko ahultasun bat.
- Beste era batzuetako 3 ahultasun.

Kritikotzat eta altutzat kalifikatutako segurtasun oharrak honi buruzkoak dira:

- Ahultasun kritiko bat aurkitu da SolMan Diagnostic Agent-en (SMDAgent), Solution Manager-ekoa (SolMan), SAP sistema bakoitzaren eta Solution Manager-en artean dauden monitorizazio eta diagnostiko gertaeren komunikazioak kudeatzen dituena. Ahultasun hau baliatuz erasotzaile batek SAP sistema osorik jar lezake arriskuan. Ahultasun horretarako CVE-2019-0330 identifikatzailea erreserbatu da.
- Testing proba automatizatuak egiteko erabiltzen den Extended Computer Aided Test Tool (eCATT) tresnan larritasun altuko ahultasun bat aurkitu da. Hori baliatuz kodea injekta liteke, eta horrela sistemaren integritatean eta eskuragarritasunean eragin. Ahultasun horretarako CVE-2019-0328 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, SAP, Ahultasuna

Zerbitzuaren ukapena Cisco ASA eta FTDren TLS eta SSL kontrolatzaile kriptografikoan

Argitalpen data: 2019/07/11

Garrantzia: Handia

Kaltetutako baliabideak:

- ASA 5506-X,
- ASA 5506-X, FirePOWER Services-ekin,
- ASA 5506H-X,
- ASA 5506H-X, FirePOWER Services-ekin,
- ASA 5506W-X,
- ASA 5506W-X, FirePOWER Services-ekin,
- ASA 5508-X,
- ASA 5508-X, FirePOWER Services-ekin,
- ASA 5516-X,
- ASA 5516-X, FirePOWER Services-ekin.

zifratzeko eta deszifratzeko kontrolatzaile kriptografiko jakin bat erabiltzen duten ASA hardwareko plataformei. Hainbat ezaugarri gaitzen direnean Cisco ASA edo FTD softwareak SSL/TLS paketeak prozesa ditzan eragiten dute. Ezaugarri horiek honakoak dira, besteak beste:

- AnyConnect eta Clientless SSL VPN,
- HTTP server, kudeaketaren interfazerako erabilita.

Azalpena:

Cisco Adaptive Security Appliance (ASA) eta Firepower Threat Defense (FTD) softwarerako kontrolatzaile kriptografikoak duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek gailua abiaraz lezake ustekabean.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak hemendik deskarga daitezke: Cisco Softwarearen deskarga panela.

Xehetasuna:

- Secure Sockets Layer (SSL) edo Transport Layer Security-ren (TLS) sarrera paketearen goiburu baten sarrera egiaztapen ez-nahikoa baliatuz, erasotzaile batek xede den gailuan sortutako interfazera TLS/SSL pakete bat bidal lezake, gailua birkargatuz. Ondorioz zerbitzuaren ukapen egoera (DoS) eragingo litzateke. Ahultasun horretarako CVE-2019-1873 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun Citrix SD-WAN-en

Argitalpen data: 2019/07/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Todas las versiones de NetScaler SD-WAN 9.x;
- Todas las versiones de NetScaler SD-WAN 10.0.x, anteriores a 10.0.8;
- Todas las versiones de Citrix SD-WAN 10.1.x;
- Todas las versiones de Citrix SD-WAN 10.2.x, anteriores a 10.2.3.

Azalpena:

Hainbat ahultasun aurkitu dira Citrix SD-WAN Center, NetScaler SD-WAN Center, Citrix SD-WAN Appliance eta NetScaler SD-WAN Appliance-n. Ahultasun horiek denek batera eragin lezakete autentifikatu gabeko erasotzaile batek root modura komandoak exekutatu ahal izatea SD-WAN Center-en kudeaketa kontsolaren aurka, edo bestela erabil litezke root pribilegioak lortzeko SD-WAN Appliance-n.

Konponbidea:

- Actualizar a la versión 10.0.8 de NetScaler SD-WAN Center y NetScaler SD-WAN Appliance.
- Actualizar a la versión 10.2.3 de Citrix SD-WAN Center y Citrix SD-WAN Appliance.

Xehetasuna:

Aurkitutako ahultasunak honakoak dira:

- Autentifikatu gabeko komandoen injekzioa Citrix SD-WAN Center-en, 10.2.3 baino lehenagoko 10.2.x bertsioak, eta NetScaler SD-WAN Center-en, 10.0.8 baino lehenagoko 10.0.x bertsioak. Ahultasun horretarako CVE-2019-12985, CVE-2019-12986, CVE-2019-12987 eta CVE-2019-12988 identifikatzaileak erreserbatu dira.
- Direktorio jauzia fitxategiak idaztean Citrix SD-WAN Center-en, 10.2.3 baino lehenagoko 10.2.x bertsioak, eta NetScaler SD-WAN Center-en, 10.0.8 baino lehenagoko 10.0.x bertsioak.Ahultasun horretarako CVE-2019-12990 identifikatzailea erreserbatu da.
- Autentifikatutako komandoen injekzioa Citrix SD-WAN Center-en, 10.2.3 baino lehenagoko 10.2.x bertsioak, eta NetScaler SD-WAN Center-en, 10.0.8 baino lehenagoko 10.0.x bertsioak.Ahultasun horretarako CVE-2019-12992 identifikatzailea erreserbatu da.
- Autentifikatu gabeko SQL injekzioa Citrix SD-WAN Appliance-n, 10.2.3 baino lehenagoko 10.2.x bertsioak, eta NetScaler SD-WAN Appliance-n, 10.0.8 baino lehenagoko 10.0.x bertsioak.Ahultasun horretarako CVE-2019-12989 identifikatzailea erreserbatu da.
- Autentifikatutako komandoen injekzioa Citrix SD-WAN Appliance-n, 10.2.3 baino lehenagoko 10.2.x bertsioak, eta NetScaler SD-WAN Appliance-n, 10.0.8 baino lehenagoko 10.0.x bertsioak.Ahultasun horretarako CVE-2019-12991 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Joomla! 3.9.10en segurtasun eguneraketa

Argitalpen data: 2019/07/11

Garrantzia: Txikia

Kaltetutako baliabideak:

Joomla! CMS, 3.9.7tik 3.9.9 bitarteko bertsioak.

Azalpena:

Joomla!-k bertsio berri bat argitaratu du, bere nukleoak duen kritikotasun txikiko ahultasun bat konpontzen duena, kodearen urruneko exekuzioarena, eta baita beste ahultasun bat ere, 3.9.9 bertsioan sartutakoa.

Konponbidea:

3.9.10 bertsiora eguneratzea.

Xehetasuna:

Kodearen urruneko exekuzio erako ahultasun hau iragazte desegoki batez baliatzen da, baimendutako erabiltzaileei eremu pertsonalizatuak sortzea ahalbidetzen diena iragazte aukerak manipulatzeko eta baliozkotu gabeko aukera bat injektatzeko. Gainera, 3.9.10 bertsioak beste ahultasun bat ere konpontzen du, 3.9.9 bertsioan sartutakoa, webgune eleaniztunetan txantiloien estiloei eragiten ziena.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun Juniper-en

Argitalpen data: 2019/07/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Juniper Networks Junos OS, 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 16.1, 16.2, 17.1, 17.2, 17.2X75, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4 eta 19.1 bertsioak;
- Steel Belted Radius Carrier Edition, 8.4 eta 8.5 bertsioak;
- Juniper Secure Analytics (JSA) Series;
- Junos Space, 19.2R1 baino lehenagoko bertsioak.

Kaltetutako bertsioen xehetasun gehiago ikusteko, erreferentzien atala kontsultatu.

Azalpena:

Juniper-ek hainbat ahultasunen berri eman du, bere produktu hauei eragiten dietenak: Juniper Networks Junos OS, Steel Belted Radius Carrier Edition, Juniper Secure Analytics (JSA) Series eta Junos Space.

Konponbidea:

Kaltetutako produktuak eguneratzea: https://www.juniper.net/support/downloads/

Xehetasuna:

Asmo gaiztoko erabiltzaile batek aipatutako ahultasunak baliatuko balitu, kaltetutako produktuetan honako ekintza hauek egin litzake:

- zerbitzuaren ukapena (DoS),
- kodearen urruneko exekuzioa,
- babes kriptografikoko mekanismoak saihestu,

- HTTPS saioetan datuak txertatu, eta seguruenik SSL edo TLS bidez babestutako beste saio mota batzuetan ere,
- ziurtagiriak faltsutu,
- SSL zerbitzari arbitrarioak faltsutu,
- BKS-V1 keystore-ren integritatea arriskuan jarri,
- gako pribatuari buruzko xehetasunak ezagutzera eman,
- sinatutako egitura batean datu "ikusezinak" sartu,
- sinaduraren k balioari buruzko informazioa lortu eta, azkenik, baita balio pribatuari buruzkoa ere,
- gako pribatuak eskuratu,
- bereizketa eta berreskuratze erasoak egin testu lauan,
- babes kriptografikorako mekanismoa gainditu eta autentifikazio gako bat aurkitu,
- pribilegioak lortu edo horien eskalatzea egin,
- erabiltzaileak zerrendatu,
- PKCS#11 modulu lokal arbitrarioak exekutatu,
- gako pribatutik informazio sentikorra eskuratu,
- zerbitzua ustekabean itxi,
- Junos Os-en veriexec murrizpenak gainditu,
- informazioa zabaldu,
- konexio hori berrerabil dadin eragin, maiuskulen /minuskulen artean bereizten ez duen pasahitz zuzenaren bertsioa ezagutzen badu,
- osokoak gainezkatu eta mugez kanpo irakurri,
- libcurl-ek memoria dinamikoan (heap) oinarritutako bere bufferretik kanpo idatz dezan eragin,
- sare transferentziako eskaerak bidali host okerrera.

Ahultasun horietara lotutako identifikatzaileen zerrendak honako hauek dira:

- Erreserbatuak:
  - Kritikoak eta altuak: CVE-2019-0049, CVE-2019-0052 y CVE-2019-0053.
  - Ertainak eta baxuak: CVE-2019-0046 y CVE-2019-0048.
- Esleituak:
  - Kritikoak eta altuak: CVE-2016-1951, CVE-2014-1545, CVE-2013-5607, CVE-2018-1000613, CVE-2018-1000180, CVE-2018-5382, CVE-2016-1000352, CVE-2016-1000344, CVE-2016-1000342, CVE-2016-1000340, CVE-2016-1000338, CVE-2015-8325, CVE-2016-6515, CVE-2016-10009, CVE-2016-10010, CVE-2016-10012, CVE-2018-15504, CVE-2018-15505, CVE-2018-1060, CVE-2018-1061, CVE-2018-11237, CVE-2018-0732, CVE-2016-8615, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2016-8625, CVE-2018-10902, CVE-2019-5739 y CVE-2018-12327.
  - Ertainak eta baxuak: CVE-2016-1938, CVE-2009-3555, CVE-2009-2409, CVE-2009-2408, CVE-2016-1000346, CVE-2016-1000345, CVE-2016-1000341, CVE-2015-7940, CVE-2013-1624, CVE-2016-2427, CVE-2016-6210, CVE-2015-6564, CVE-2016-10011, CVE-2019-1559, CVE-2018-1729, CVE-2018-0739, CVE-2016-8616 y CVE-2019-6133.

Etiketak: Eguneraketa, Ahultasuna

Txantiloien injekzio erako ahultasuna Atlassian-en hainbat produktutan

Argitalpen data: 2019/07/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Jira Server eta Jira Data Center, honako bertsioak:

- 4.4.0tik 7.6.14aren aurrekoa bitartekoak,
- 7.7.0tik 7.13.5aren aurrekoa bitartekoak,
- 8.0.0tik 8.0.3aren aurrekoa bitartekoak,
- 8.1.0tik 8.1.2aren aurrekoa bitartekoak,
- 8.2.0tik 8.2.3aren aurrekoa bitartekoak.

Azalpena:

Daniil Dmitriev ikertzaileak larritasun kritikoko ahultasun bat aurkitu du, zerbitzariaren aldeko txantiloien injekzio erakoa. Hori baliatuz kodea exekuta liteke urrunetik.

Konponbidea:

Ondoko bertsioetara eguneratzea:

- 7.6.14,
- 7.13.5,
- 8.0.3,
- 8.1.2,
- 8.2.3.

Xehetasuna:

Zerbitzariaren aldeko txantiloien injekzio erako ahultasun bat baliatuz, erasotzaile batek kodearen urruneko exekuzioa egin lezake. Ahultasun horretarako CVE-2019-11581 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Squid-en

Argitalpen data: 2019/07/15

Garrantzia: Handia

Kaltetutako baliabideak:

- Squid-en kaltetutako bertsioak:
  - 2.x adarra, bertsio guztiak;3.x adarra,
  - 3.5.28 bertsiora bitartean;4.x adarra,
  - 4.7 bertsiora bitartean.

Azalpena:

Bost ahultasun aurkitu dira Squid proxy zerbitzariaren hainbat bertsiotan.

Konponbidea:

Ahultasunak konpontzeko, 4.8 bertsiora eguneratzea.

Xehetasuna:

- Aurkitutako ahultasunak baliatuz urruneko erasotzaile batek honakoa egin lezake:
  - informazioa lapurtu,
  - kodea exekutatu eta
  - zerbitzuaren ukapen egoera eragin.

Ahultasun horietarako CVE-2019-12854, CVE-2019-12529, CVE-2019-12525, CVE-2019-12527 eta CVE-2019-13345 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Ahultasuna

Eguneraketa kritikoak Oraclen (2019ko uztaila)

Argitalpen data: 2019/07/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Application Express, 5.1, 18.2 bertsioak;
- Diagnostic Assistant, 2.12.36 baino lehenagoko bertsioak;
- Enterprise Manager Base Platform, 12.1.0.5.0, 13.2.0.0.0, 13.3.0.0.0 bertsioak;
- Enterprise Manager for Fusion Middleware, 13.2, 13.3 bertsioak;
- Enterprise Manager for Virtualization, 13.1, 13.2, 13.3 bertsioak;
- Enterprise Manager Ops Center, 12.3.3, 12.4.0 bertsioak;
- Instantis EnterpriseTrack, 17.1, 17.2, 17.3 bertsioak;
- JD Edwards EnterpriseOne Tools, 9.2 bertsioa;
- JD Edwards World Security, A9.3, A9.3.1, A9.4 bertsioak;
- MICROS Retail XBRi Loss Prevention, 10.8.0 - 10.8.3 bertsioak;
- MICROS Retail-J, 12.1.0, 12.1.1, 12.1.2, 13.1 bertsioak;
- MySQL Enterprise Monitor, 4.0.9 eta lehenagoko bertsioak, 8.0.14 eta lehenagokoak;
- MySQL Server, 5.6.44 eta lehenagoko bertsioak, 5.7.26 eta lehenagokoak, 8.0.16 eta
- lehenagokoak;
- MySQL Workbench, 8.0.16 eta lehenagoko bertsioak;
- Oracle Agile Engineering Data Management, 6.2.0, 6.2.1 bertsioak;
- Oracle Agile PLM, 9.3.3, 9.3.4, 9.3.5, 9.3.6 bertsioak;
- Oracle Application Testing Suite, 13.1, 13.2, 13.3 bertsioak;
- Oracle Banking Platform, 2.4.0 - 2.7.1 bertsioak;
- Oracle Berkeley DB, honako bertsioak: 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23, 12.1.6.2.32;
- Oracle BI Publisher, 11.1.1.9.0 bertsioa;
- Oracle Business Intelligence Enterprise Edition, 11.1.1.9.0, 12.2.1.4.0 bertsioak;
- Oracle Clusterware, 12.1.0.2.0 bertsioa;
- Oracle Communications Application Session Controller, 3.7.1 eta 3.8.0 bertsioak;
- Oracle Communications Billing and Revenue Management, 7.5, 12.0 bertsioak;
- Oracle Communications Converged Application Server, 5.1, 7.0, 7.1 bertsioak;
- Oracle Communications Converged Application Server - Service Controller, 6.0, 6.1 bertsioak;
- Oracle Communications Convergence, 3.0.2 bertsioa;
- Oracle Communications Diameter Signaling Router (DSR), 8.0, 8.1, 8.2, 8.3 bertsioak;
- Oracle Communications EAGLE (Software), 46.5, 46.6, 46.7 bertsioak;
- Oracle Communications Instant Messaging Server, 10.0.1.2.0 bertsioa;
- Oracle Communications Interactive Session Recorder, 6.0, 6.1 eta 6.2 bertsioak;
- Oracle Communications Messaging Server, 8.0.2 eta 8.1.0 bertsioak;
- Oracle Communications Online Mediation Controller, 6.1 bertsioa;
- Oracle Communications Unified, 8.0.0.2.0 bertsioa;
- Oracle Data Integrator, 12.2.1.3.0 bertsioa;
- Oracle Database Server, 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c eta 19c bertsioak;
- Oracle Demantra Demy Management, 7.3.1.5.2 bertsioa;
- Oracle E-Business Suite, 12.1.1 - 12.1.3, 12.2.3 - 12.2.8 bertsioak;
- Oracle Endeca Information Discovery Integrator, 3.2.0 bertsioa;
- Oracle Endeca Server, 7.7.0 bertsioa;
- Oracle Enterprise Manager Base Platform, 12.1.0.5.0, 13.2.0.0.0, 13.3.0.0.0 bertsioak;
- Oracle Enterprise Repository, 12.1.3.0.0 bertsioa;
- Oracle Financial Services - Regulatory Reporting for Reserve Bank of India - Lombard Risk Integration Pack, 8.0.7 bertsioa;
- Oracle Financial Services - Regulatory Reporting for US Federal Reserve - Lombard Risk Integration Pack, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Analytical Applications Infrastructure, 7.3.3 - 7.3.5 eta 8.0.2 - 8.0.8 bertsioak;
- Oracle Financial Services Analytical Applications Reconciliation Framework, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Asset Liability Management, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Basel Regulatory Capital Basic, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Data Foundation, 8.0.4 - 8.0.8 bertsioak;
- Oracle Financial Services Data Integration Hub, 8.0.5 - 8.0.7 bertsioak;
- Oracle Financial Services Funds Transfer Pricing, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Hedge Management eta IFRS Valuations, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Institutional Performance Analytics, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Liquidity Risk Management, 8.0.1, 8.0.2, 8.0.4, 8.0.5, 8.0.6 bertsioak;

- Oracle Financial Services Liquidity Risk Management, 8.0.7, 8.0.8 bertsioak;
- Oracle Financial Services Loan Loss Forecasting and Provisioning, 8.0.2 - 8.0.7 bertsioak;
- Oracle Financial Services Market Risk Measurement and Management, 8.0.5, 8.0.6, 8.0.8 bertsioak;
- Oracle Financial Services Price Creation and Discovery, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Profitability Management, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Regulatory Reporting for European Banking Authority, 8.0.6, 8.0.7 bertsioak;
- Oracle Financial Services Regulatory Reporting for European Banking Authority - Integration Pack for Lombard Risk, 8.0.6, 8.0.7 bertsioak;
- Oracle Financial Services Regulatory Reporting for US Federal Reserve, 8.0.4 - 8.0.7 bertsioak;
- Oracle Financial Services Retail Customer Analytics, 8.0.4 - 8.0.6 bertsioak;
- Oracle Financial Services Revenue Management and Billing, 2.4.0.0, 2.4.0.1 bertsioak;
- Oracle FLEXCUBE Core Banking, 5.2.0, 11.6.0, 11.7.0, 11.8.0 bertsioak;
- Oracle FLEXCUBE Enterprise Limits and Collateral Management, 12.0, 12.1 bertsioak;
- Oracle FLEXCUBE Investor Servicing, 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0, 14.1.0 bertsioak;
- Oracle FLEXCUBE Private Banking, 12.0.1, 12.0.3, 12.1.0 bertsioak;
- Oracle FLEXCUBE Universal Banking, 12.0.1 - 12.0.3, 12.1.0 - 12.4.0, 14.0.0 - 14.2.0 bertsioak;
- Oracle Global Lifecycle Management OPatchAuto, 12.2.0.1.14 baino lehenagoko bertsioak;
- Oracle GraalVM Enterprise Edition, 19.0.0 bertsioa;
- Oracle Hospitality Gift and Loyalty, 9.0.0, 9.1.0 bertsioa;
- Oracle Hospitality Guest Access, 4.2, 4.2.1 bertsioak;
- Oracle Hospitality Simphony, 18.2.1 bertsioa;
- Oracle Hospitality Suite8, 8.9.6, 8.10.2, 8.11 - 8.14 bertsioak;
- Oracle HTTP Server, 12.1.3.0.0, 12.2.1.3.0 bertsioak;
- Oracle Hyperion Planning, 11.1.2.4 bertsioa;
- Oracle Hyperion Workspace, 11.1.2.4 bertsioa;
- Oracle Identity Manager, 11.1.2.3.0, 12.2.1.3.0 bertsioak;
- Oracle Insurance Allocation Manager for Enterprise Profitability, 8.0.8 bertsioa;
- Oracle Insurance Calculation Engine, 9.7, 10.0, 10.1, 10.2 bertsioak;
- Oracle Insurance Data Foundation, 8.0.4 - 8.0.7 bertsioak;
- Oracle Insurance IFRS 17 Analyzer, 8.0.6, 8.0.7 bertsioak;
- Oracle Insurance Performance Insight, 8.0.7 bertsioa;
- Oracle Insurance Policy Administration J2EE, 10.0, 10.1, 10.2, 11.0 bertsioak;
- Oracle Insurance Rules Palette, 10.0, 10.1, 10.2, 11.0 bertsioak;
- Oracle Java SE, 7u221, 8u212, 11.0.3, 12.0.1 bertsioak;
- Oracle Java SE Embedded, 8u211 bertsioa;
- Oracle Outside In Technology, 8.5.4 bertsioa;
- Oracle Retail Advanced Inventory Planning, 15.0 bertsioa;
- Oracle Retail Customer Management and Segmentation Foundation, 16.0, 17.0, 18.0 bertsioak;
- Oracle Retail Financial Integration, 14.0, 14.1, 15.0, 16.0 bertsioak;
- Oracle Retail Integration Bus, 15.0, 16.0 bertsioak;
- Oracle Retail Order Broker, 5.2, 15.0 bertsioak;
- Oracle Retail Order Management System, 5.0 bertsioa;
- Oracle Retail Predictive Application Server, 14.0.3.26, 14.1.3.37, 15.0.3.100, 16.0 bertsioak;
- Oracle Retail Service Backbone, 16.0.1 bertsioa;
- Oracle Retail Back Office, 7.0, 7.1 bertsioak;
- Oracle Retail Xstore Point of Service, 7.0, 7.1, 15.0, 16.0, 17.0, 18.0 bertsioak;
- Oracle Security Service, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0 bertsioak;
- Oracle SOA Suite, 12.2.1.3.0 bertsioa;
- Oracle Solaris, 10, 11.3, 11.4 bertsioak;
- Oracle Transportation Management, 6.3.7 bertsioa;
- Oracle Utilities Advanced Spatial and Operational Analytics, 2.7.0.1 bertsioa;
- Oracle Utilities Framework, 4.3.0.2.0 - 4.3.0.6.0, 4.4.0.0.0 bertsioak;
- Oracle VM VirtualBox, 5.2.32 baino lehenagoko bertsioak, 6.0.10 baino lehenagokoak;
- Oracle WebCenter Sites, 12.2.1.3.0 bertsioa;
- Oracle WebLogic Server, 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 bertsioa;
- PeopleSoft Enterprise FIN Project Costing, 9.2 bertsioa;
- PeopleSoft Enterprise PeopleTools, 8.55, 8.56, 8.57 bertsioak;
- PeopleSoft Enterprise PT PeopleTools, 8.55, 8.56, 8.57 bertsioak;
- Primavera Analytics, 18.8 bertsioa;
- Primavera Gateway, 15.2, 16.2, 17.12, 18.8 bertsioak;
- Primavera Unifier, 16.1, 16.2, 17.7 - 17.12 eta 18.8 bertsioak;
- Services Tools Bundle, 19.2 bertsioa;
- Siebel Applications, 19.0 eta lehenagoko bertsioak;
- StorageTek Tape Analytics SW Tool, 2.3.0 bertsioa;
- Sun ZFS Storage Appliance Kit (AK), 8.8.3 bertsioa;
- System Utilities, 19.1 bertsioa;
- Tape Virtual Storage Manager GUI, 6.2 bertsioa.

Azalpena:

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

Konponbidea:

Kaltetutako produktuen arabera, dagozkien partxeak aplikatzea. Eguneraketak deskargatzeko informazioa Oraclek argitaratutako segurtasun buletinean lor daiteke.

Xehetasuna:

Eguneraketa horrek 319 ahultasun konpontzen ditu guztira, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna Erreferentzien atalean dagoen Oracleren loturan kontsulta daiteke.

Etiketak: Eguneraketa, Java, Oracle, Birtualizazioa, Ahultasuna

---

Segurtasuna saihestearen erako ahultasuna Windows Defender Application Control-en (WDAC)

Argitalpen data: 2019/07/17

Garrantzia: Handia

Kaltetutako baliabideak:

- PowerShell Core, 6.1 eta 6.2 bertsioak.

Azalpena:

Microsoftek PowerShell Core produktuari eragiten zion zikloz kanpoko ahultasun bat konpondu du.

Konponbidea:

- PowerShell Core 6.1 bertsioaren kasuan, 6.1.5 bertsiora eguneratzea
- PowerShell Core 6.2 bertsioaren kasuan, 6.2.2 bertsiora eguneratzea

Xehetasuna:

Windows Defender Application Control-ek (WDAC) duen segurtasuna saihestearen erako ahultasun bat baliatuz, administratzaile baimenak dituen erasotzaile batek PowerShell Core-ren lengoaiaren modu murriztua saihets lezake, eta baliabideetara sarbidea lortu nahi gabe. Ahultasun horretarako CVE-2019-1167 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Microsoft, Ahultasuna

Sarbidearen saiheste erako ahultasuna Drupal-en core-an

Argitalpen data: 2019/07/18

Garrantzia: Handia

Kaltetutako baliabideak:

8.7.4 bertsioa.

Azalpena:

Sarbidearen saiheste erako ahultasun bat aurkitu da Drupal-en core-an.

Konponbidea:

Webgunea Drupal 8.7.4 exekutatzen ari bada, 8.7.5 bertsiora eguneratzea. Workspaces modulua gaituta duten webguneen kasuan, update.php fitxategia exekutatu beharra dago cachearen garbiketa beharrezkoa bermatzeko. Alderantzizko proxy-aren cachea edo edukien hedapen sare bat (CDN) baldin badago, gomendagarria da horietan cachearen garbiketa egitea ere.

Xehetasuna:

Drupal 8.7.4en, Workspaces modulu esperimentala aktibatzen denean, sarbidearen saiheste egoera sortzen da. Ahultasun horretarako CVE-2019-6342 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun Jenkins-en

Argitalpen data: 2019/07/18

Garrantzia: Handia

Kaltetutako baliabideak:

- Jenkins Weekly, 2.185 eta lehenagoko bertsioak.
- Jenkins LTS, 2.176.1 eta lehenagoko bertsioak.

Azalpena:

Jenkins-ek 3 ahultasunen berri eman du, bat kritikotasun altukoa eta bi ertainekoak. Ahultasun horietako bat arrakastaz baliatuz gero *Cross-site request forgery* (CSRF) erako erasoak egin litezke, fitxategiak modu arbitrarioan idatzi, edo baimenik gabeko sarbidea lortu atalen ikuspegira.

Konponbidea:

- Jenkins Weekly, 2.186 bertsiora eguneratzea.
- Jenkins LTS, 2.176.2 bertsiora eguneratzea.

Xehetasuna:

- Larritasun altuko ahultasunaren arrazoia da Jenkins-en tokenek soilik egiaztatzen dituztela erabiltzailearen autentifikazioa eta IP helbidea. Hori baliatuz erasotzaile batek beste erabiltzaile baten tokena eskura lezake eta Cross-site request forgery (CSRF) erasoak egin, baldin eta biktimaren IP helbidea aldatzen ez bada. Ahultasun horretarako CVE-2019-10353 identifikatzailea erabili da.
- Gainerako ahultasunetarako honako identifikatzaileak esleitu dira: CVE-2019-10352 eta CVE-2019-10354.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Cisco gailuetan

Argitalpen data: 2019/07/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco Vision Dynamic Signage Director, honako bertsioak:
  - 5.0 eta lehenagokoak;
  - 6.0;
  - 6.1.
- Cisco FindIT Network Manager eta Cisco FindIT Network Probe 1.1.4 bertsioa, Ciscok emandako irudi birtualak erabiltzen badituzte.
- Cisco IOS Access Points Major Software, 802.11r FTrako konfiguratuta, honako bertsioak:
  - 8.0eta lehenagokoak;
  - 8.1;
  - 8.2;
  - 8.3;
  - 8.4;
  - 8.5;
  - 8.6;
  - 8.7.

Azalpena:

Ciscok bere hainbat produkturi eragiten dieten hiru ahultasun aurkitu ditu, bat larritasun kritikokoa eta beste bi larritasun altukoak. Autentifikaziorik gabeko urruneko erasotzaile batek autentifikazioa saihets lezake, kontu batera sartu root pribilegioekin edo zerbitzuaren ukapen egoera eragin.

Konponbidea:

- Cisco Vision Dynamic Signage Director, honako bertsioak: :
  - 5.0 eta lehenagokoak, 5.0sp9ra eguneratzea;
  - 6.0 eta 6.1, 6.1sp3ra eguneratzea.
- Cisco FindIT Network Manager eta Cisco FindIT Network Probe 1.1.4 bertsioa, 2.0 bertsiora eguneratzea.
- Cisco IOS Access Points Major Software, 802.11r FTrako konfiguratuta:
  - 8.0 eta lehenagoko bertsioen eta 8.1 eta 8.2 bertsioen kasuan, 8.2.170.0 bertsiora eguneratzea;
  - 8.3 bertsioaren kasuan, 8.3.150.0 bertsiora eguneratzea;
  - 8.4 eta 8.5 bertsioen kasuan, 8.5.131.0 bertsiora eguneratzea;
  - 8.6 eta 8.7 bertsioen kasuan, 8.8.100.0 bertsiora eguneratzea.

Xehetasuna:

- Larritasun kritikoko ahultasunak Cisco Vision Dynamic Signage Director Software-ren REST APIari eragiten dio. Honen arrazoia da HTTP eskaeren baliozko ez-nahiko bat. Autentifikaziorik gabeko urruneko erasotzaile batek bereziki sortutako HTTP pakete bat bidal lezake, eta horrela sisteman ekintza arbitrarioak egin administratzaile pribilegioekin. Ahultasun horretarako CVE-2019-1917 identifikatzailea erabili da.
- Larritasun altuko ahultasun baten arrazoia da azpiko Linux sistema eragilean kontu bat egotea kredentzial estatikoekin. Erasotzaile batek sarbidea lor lezake kontu horretara, root pribilegioak dituena. Ahultasun horretarako CVE-2019-1919 identifikatzailea erabili da.
- Larritasun altuko beste ahultasunaren arrazoia da FTrako konfiguratutako interfazera bezeroak bidalitako autentifikazio eskaeretan akatsak maneiatzeko baldintzan dagoen erabateko gabezia. Alboko erasotzaile batek interfazerako bereziki diseinatutako autentifikazio eskaera bidal lezake, eta horrela zerbitzuaren ukapen egoera sor lezake (DoS). Ahultasun horretarako CVE-2019-1920 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Kodearen urrutiko exekuzioaren ahultasuna, Palo Alto PAN-OS

Argitalpen data: 2019/07/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- PAN-OS 7.1.18 eta aurrekoak.
- PAN-OS 8.0.11 eta aurrekoak.
- PAN-OS 8.1.2 eta aurrekoak.

Deskribapena:

Palo Alto sistemak larritasun kritikoko ahultasun bat argitaratu du. Horren ondorioz, egiaztatu gabeko erasotzaile batek kode arbitrarioa exekutatu lezake.

Konponbidea:

Palo Alto sistemak honako bertsioetara eguneratuko ditu bere produktuak:

- PAN-OS 7.1.19 edo hortik gorakoa.
- PAN-OS 8.0.12 edo hortik gorakoa.
- PAN-OS 8.1.3 edo hortik gorakoa.

Xehetasuna:

Ahultasunak, kodearen urrutiko exekuzioak (RCE), kode arbitrarioa exekutatzeko aukera eman liezaioke egiaztu gabeko erasotzaile bati. Ahultasun horretarako, CVE-2019-1579 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasunak ProFTPD zerbitzarietan

Argitalpen data: 2019/07/25

Garrantzia: Kritikoa

Kaltetutako baliabideak:

1.3.6 bertsioa eta aurrekoak.

Deskribapena:

Tobias MÃ¤del ikertzaileak larritasun kritikoko ahultasun bat atzeman du ProFTPD zerbitzarien mod_copy moduluan. Egiaztatu gabeko urrutiko erasotzaile batek kodea exekutatu lezake, edota informazioa argitaratu.

Konponbidea:

Ez da konponbiderik argitaratu bertsio berri edo eguneraketa moduan, ahultasun hori konpontzeko. Eguneraketa noiz iragarriko zain egoteko gomendatu dute.

- Neurri aringarri moduan, mod_copy modulua desgaitzeko gomendioa egin da.
- Git gordailuaren Bug Tracker delakoan kontsulta daitekeen zuzenketa garatu da..
- Debian-en kasuan, 1.3.6-6 ez egonkorrerako soilik balio duen partxe bat diseinatu da (Release sid).

Xehetasuna:

Mod_copy moduluko ahultasunak, direktorioen arteko artxiboen kopiak kudeatzeaz arduratzen denak, erasotzaile bati aukera eman diezaioke, egiaztatu gabe, kodea exekutatu edota informazioa argitaratzeko. Ahultasun horretarako, CVE-2019-12815 identifikatzailea esleitu da.

Etiketak: Linux, Ahultasuna

Network Time Protocol (NTP) sistemaren ahultasuna

Argitalpen data: 2019/07/25

Garrantzia: Handia

Kaltetutako baliabideak:

- F5 produktorea:
  - BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), bertsioak:
    - 15.0.0;
    - 14.0.0tik 14.1.0ra;
    - 13.1.0tik 13.1.1ra;
    - 12.1.0tik 12.1.4ra;
    - 11.5.2tik 11.6.4ra;
  - Enterprise Manager. 3.1.1 bertsioa;
  - BIG-IQ Centralized Management:
    - 6.0.0tik 6.1.0ra;
    - 5.1.0tik 5.4.0ra;
  - F5 iWorkflow, 2.3.0 bertsioa;
  - Traffix SDC, 5.0.0tik 5.1.0ra.
- Red Hat Enterprise, 5, 6 eta 7 bertsioak.

Deskribapena:

Kritikotasun handiko ahultasun bat atzeman da, NTP protokoloa falta zaiona. Urrutiko erasotzaile batek baliabideak eskura litzake, artxiboak aldatu, edota sisteman zerbitzu ukapen bat sortu.

Konponbidea:

Ezin izan da eguneraketa horretarako partxe edo eguneraketa bidezko konponbiderik eman. Ahultasuna arintzeko jarraibiderik ere ez da argitaratu; hori dela eta, eguneraketa posible baten zain geratzen gara.

Xehetasuna:

Network Time Protocol (NTP) sistemak, RFC 5905 delakoan azaltzen den moduan, 123 portua erabiltzen du portu finkoko zenbaki bat eskatzen ez den moduetarako ere. Horrek ibilbidez kanpoko erasoak egiteko aukera ematen die urrutiko erasotzaileei. Urrutiko erasotzaile batek baliabideak eskura litzake, artxiboak aldatu, edota sisteman zerbitzu ukapen bat sortu. Ahultasun horretarako CVE-2019-11331 identifikatzailea esleitu da.

Etiketak: Linux, Ahultasuna

XXE injekzio erasoa IBM erakundearen Daeja ViewONE sisteman

Argitalpen data: 2019/07/29

Garrantzia: Handia

Kaltetutako baliabideak:

Daeja ViewONE Virtual, 5.0 eta 5.0.6 bertsioen bitartekoak.

Deskribapena:

IBM enpresak kritikotasun handiko ahultasun bat atzeman du Daeja ViewONE Professional, Standard eta Virtual sistemetan. Urrutiko erasotzaile batek informazio sentikorra argitara dezake edota zerbitzuaren ukapen baldintza bat sortu.

Konponbidea:

IBMk bi partxe argitaratu ditu ahultasuna konpontzeko:

- Daeja ViewONE Virtual 5.0.5 iFix 14
- Daeja ViewONE Virtual 5.0.6 iFix 2

Xehetasuna:

Daeja ViewONE Virtual sistema XML External Entity (XXE) injekzio eraso baten eraginpean egon daiteke, XML datuak prozesatzean. Urrutiko erasotzaile batek informazio sentikorra argitara dezake, edota memoria baliabideak kontsumitu, eta zerbitzuaren ukapen baldintza bat ere sor liteke. Ahultasun horretarako, CVE-2019-4456 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, IBM, Ahultasuna