2019ko Martxoaren Bulletina

Ohartarazpenak - Teknikoak

Birbideratze irekiaren ahultasuna IBMren hainbat produktutan

Argitalpen data: 2019/03/04

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM InfoSphere Information Governance Catalog, 11.3, 11.5 eta 11.7 bertsioak
- IBM InfoSphere Information Server on Cloud, 11.5 eta 11.7 bertsioak

Azalpena:

IBM InfoSphere Information Server-ek urruneko erasotzaile bati phishing erasoak egitea ahalbidetu liezaioke, birbideratze irekiko eraso bat erabiliz.

Konponbidea:

- Bi produktuetan 11.7 bertsioaren kasuan:
  - 1.7.0.2 bertsiora eguneratzea eta ondoren 11.7.0.2 Service Pack 1 bertsiora eguneratzea.
- Bi produktuetan 11.5 bertsioaren kasuan:
  - 11.5.0.2 bertsiora eguneratzea eta ondoren 11.5 Service Pack 5 bertsiora eguneratzea.
- IBM InfoSphere Information Governance Catalog 11.3 bertsioaren kasuan, bertsio berrienera eguneratzea.

Xehtasuna:

- IBM InfoSphere Information Server-ek urruneko erasotzaile bati phishing erasoak egitea ahalbidetu liezaioke, birbideratze irekiko eraso bat erabiliz. Biktima bat konbentzitu ondoren bereziki diseinatutako webgune bat bisita dezan, urruneko erasotzaile batek ahultasun hau balia lezake erakutsitako URLa faltsutzeko eta erabiltzaile bat fidagarria zirudien webgune gaizto batera birbideratzeko. Horri esker erasotzaileak informazio oso sentikorra eskura lezake edo biktimaren aurkako eraso berriak egin. Ahultasun horretarako CVE-2018-1875 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Ahultasunak Apache-ren JMeter eta Qpid Broker-Jn

Argitalpen data: 2019/03/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Qpid Broker-J, 6.0.0tik 7.0.6ra bitarteko bertsioak eta 7.1.0 bertsioa

Azalpena:

Apache-ren JMeter eta Qpid Broker-Jk dituzten ahultasunak baliatuz, kodearen urruneko exekuzioa eta zerbitzuaren ustekabeko itxiera eragin litezke.

Konponbidea:

- JMeter-en kasuan: azken bertsiora (5.1) eguneratzea eta SSL RMI konexio autentifikatua erabiltzea (modu lehenetsian gaituta). Horrez gain, eskuragarri dagoen azken java bertsioa erabiltzea (8tik 11ra bitartekoa).
- Apache Qpid Broker-Jren kasuan: Qpid Broker-Jren 7.0.7 edo 7.1.1 edo bertsio berriagoetarako eguneratzea.

Xehetasuna:

- Autentifikaziorik gabeko erasotzaile batek RMI konexio bat ezar lezake JMeter-en zerbitzari batera RemoteJMeterEngine erabiliz. Horrela eraso bat abiaraz lezake datu ez fidagarrien deserializazioa erabiliz. Honek soilik eragiten die modu banatuan exekutatzen diren probei. Ahultasun horretarako CVE-2019-0187 identifikatzailea erreserbatu da.
- Apache Qpid Broker-J-k duen zerbitzuaren ukapen erako ahultasun bat baliatuz, autentifikaziorik gabeko erasotzaile batek broker instantzia blokea lezake bereziki diseinatutako komandoak bidaliz, eta AMPQ protokoloaren 1.0 bertsioa baino txikiagoak erabiliz.Ahultasun horretarako CVE-2019-0200 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Apache, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/03/07

Garrantzia: Handia

Kaltetutako baliabideak:

- Firepower 4100 Series Next-Generation Firewalls
- Firepower 9300 Security Appliance
- MDS 9000 Series Multilayer Switches
- Nexus 1000V Switch for Microsoft Hyper-V y Nexus 1000V Switch para VMware vSphere
- Nexus 2000 Series Fabric Extenders
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 3600 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches, Nexus 9000 Series ACI Mode Switches que ejecuten versiones anteriores a la 14.0(3d) y Nexus 9000 Series Fabric Switches en modo Application Centric Infrastructure (ACI)
- Nexus 9500 R-Series Line Cards and Fabric Modules
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects

Azapena:

Ciscok kritikotasun altuko 26 ahultasunen berri eman du, 47 produkturi eragiten dietenak.

Konponbidea:

- Ciscok ahultasunak konpontzen dituzten hainbat konponbide argitaratu ditu, kaltetutako produktuaren arabera. Eguneraketak eskuragarri daude Ciscoren softwarearen deskargen panelean.

Xehetasuna:

Ahultasun horietako batzuk arrakastaz baliatuz gero, ondokoak eragin litezke:

- Kode arbitrarioaren exekuzioa: CVE-2019-1613, CVE-2019-1612, CVE-2019-1611, CVE-2019-1610, CVE-2019-1609, CVE-2019-1608, CVE-2019-1607, CVE-2019-1606 eta CVE-2019-1618.
- Zerbitzuaren ukapena (DoS): CVE-2019-1597, CVE-2019-1598,CVE-2019-1617, CVE-2019-1599, CVE-2019-1616 eta CVE-2019-1594.
- Kodearen urruneko exekuzioa root pribilegioekin: CVE-2019-1614.
- SEren irudiaren sinaduran egiaztapen okerra: CVE-2019-1615.
- Pribilegioen eskalatzea: CVE-2019-1604, CVE-2019-1603,CVE-2019-1596, CVE-2019-1602.
- Fitxategien sistemara baimenik gabeko sarbidea: CVE-2019-1601 eta CVE-2019-1600.
- Pribilegioen eskalatzea, beste erabiltzaile rol batzuei baimendutako kodearen exekuzioaren bidez: CVE-2019-1593.
- Kodearen exekuzio arbitrarioa root pribilegioekin: CVE-2019-1605.
- Murriztutako shell-etik ihes egitea eta kodearen exekuzio arbitrarioa root pribilegioekin kaltetutako gailuan: CVE-2019-1591.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Erabiltzailearen informazioaren hedapena TIBCOren JasperReports Server-en

Algitalpen data: 2019/03/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- TIBCO JasperReports Server, versiones 6.4.0, 6.4.1, 6.4.2, y 6.4.3
- TIBCO JasperReports Server, versión 7.1.0
- TIBCO JasperReports Server Community Edition, versiones 7.1.0 y anteriores
- TIBCO JasperReports Server para ActiveMatrix BPM, versiones 6.4.3 y anteriores
- TIBCO Jaspersoft para AWS with Multi-Tenancy, versiones 7.1.0 y anteriores
- TIBCO Jaspersoft Reporting y Analytics para AWS, versiones 7.1.0 y anteriores

Azalpena:

Source Incite-ko Steven Seeley-k (mr_me) Trend Micro Zero Day Initiative-rekin lankidetzan aurkitutako ahultasun baten berri eman du TIBCOk. Hori baliatuz autentifikaziorik gabeko erasotzaile batek JasperReports Server-en HTTP interfazearen zatien baimenen egiaztapenak saihets litzake.

Konponbidea:

- TIBCO JasperReports Server-en kasuan, 6.4.0, 6.4.1, 6.4.2, eta 6.4.3 bertsioak: 6.4.4 edo bertsio berriagora eguneratzea.
- TIBCO JasperReports Server-en kasuan, 7.1.0 bertsioa: 7.1.1 edo bertsio berriagora eguneratzea.
- TIBCO JasperReports Server Community Edition-en kasuan, 7.1.0 eta lehenagoko bertsioak: 7.1.1 edo goragoko bertsiora eguneratzea.
- ActiveMatrix BPMrako TIBCO JasperReports Server-en kasuan, 6.4.3 eta lehenagoko bertsioak: 6.4.4 edo goragoko bertsiora eguneratzea.
- AWS with Multi-Tenancy-rako TIBCO Jaspersoft-en kasuan, 7.1.0 eta lehenagoko bertsioak: 7.1.1 edo goragoko bertsiora eguneratzea.
- AWSrako TIBCO Jaspersoft Reporting eta Analytics-en kasuan, 7.1.0 eta lehenagoko bertsioak: 7.1.1 edo goragoko bertsiora eguneratzea.

Xehetasuna:

- Ahultasun horretarako CVE-2018-18815 identifikatzailea erreserbatu da. Hori baliatuz, eta CVE-2018-18809 identifikatzailea duen ahultasunarekin konbinatzen denean, erasotzaile batek host sistemaren edukietara autentifikaziorik gabeko irakurketa sarbidea lor lezake.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Bufferraren gainezkatze erako hainbat ahultasun IBMren Db2n

Argitalpen data: 2019/03/08

Garrantzia: Handia

Kaltetutako baliabideak

- IBM Db2 V9.7, V10.1, V10.5 y V11.1 en todas las plataformas.

Azalpena:.

IBMk bere IBM Db2 produktuek dituzten bufferraren gainezkatze erako hainbat ahultasunen berri eman du. Horiek baliatuz erasotzaile batek pribilegioen eskalatzea lor lezake, autentifikatutako erabiltzaile lokal batetik root-eraino edo instantziaren jaberaino.

Konponbidea:

- Dagokion partxea aplikatzea, bertsioaren eta plataformaren arabera. Deskargetarako loturak "Erreferentziak" atalean daude eskuragarri.

Xehetasuna:

- Linux, UNIX eta Windowserako IBM DB2k (DB2 Connect Server-ek barne) bufferraren gainezkatze erako hainbat ahultasunen eragina jasaten du. Horiek baliatuz:
-
    - Erasotzaile batek kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2018-1922 eta CVE-2018-1923 identifikatzaileak erreserbatu dira.
    - Erasotzaile lokal autentifikatu batek kode arbitrarioa exekuta lezake sisteman root modura. Ahultasun horretarako CVE-2018-1978, CVE-2018-1980, CVE-2018-4015 eta CVE-2018-4016 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun IBMren MQn

Argitalpen data: 2019/03/11

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM MQ V8, 8.0.0.0 - 8.0.0.10 bertsioak
- IBM MQ V9 LTS, 9.0.0.0 - 9.0.0.5 bertsioak
- IBM MQ V9.1 LTS, 9.1.0.0 - 9.1.0.1 bertsioak
- IBM MQ V9.1 CD, 9.1.0 - 9.1.1 bertsioak

Azalpena:

IBM MQk dituen hainbat ahultasunen berri eman du IBMk. Horiek baliatuz kodea exekuta liteke root pribilegioekin eta pribilegioak eskalatzea lortu.

Konponbidea:

- IBM MQ V8ren kasuan, 8.0.0.11 partxea aplikatzea
- IBM MQ V9 LTSren kasuan, IBM MQ 9.0.0.5erako iFix IT27293 aplikatzea
- IBM MQ V9.1 LTSren kasuan, IBM MQ 9.1.0.1erako iFix IT27293 aplikatzea
- IBM MQ V9.1 CDren kasuan, IBM MQ 9.1.1erakoiFix IT24586 aplikatzea

Xehetasuna:

- IBM WebSphere MQk erasotzaile lokal bati ahalbidetu liezaioke kodea injektatzea root pribilegioekin. Ahultasun horretarako CVE-2018-1998 identifikatzailea erreserbatu da.
- IBM MQk autentifikatutako erasotzaile bati ahalbidetu liezaioke pribilegioak eskalatzea kanal multiplexatuak erabiltzean. Ahultasun horretarako CVE-2018-1974 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Informazioaren hedapen erako ahultasuna Citrix-en ADM Agent-en

Argitalpen data: 2019/03/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Citrix Application Delivery Management (ADM) Agent, *build* 50.33 baino lehenagoko 12.1 bertsioa
- Citrix Application Delivery Management (ADM) Agent, *build* 33.23 baino lehenagoko 13.0 bertsioa

Azalpena:

Citrix-ek larritasun kritikoko ahultasun bat aurkitu du Application Delivery Management (ADM) bere produktuan. Hori baliatuz informazio sentikorra eskura liteke eta horrekin pribilegioak eskalatzea lortu.

Konponbidea:

Ahultasun hori konpondua izan da ondoren aipatzen diren bertsioetan, beren deskargen zentroan eskuragarri:

- Citrix Application Delivery Management Agent, *build* 50.33en 12.1 bertsioa eta ondorengoak.
- Citrix Application Delivery Management Agent Cloud, *build* 33.23en 13.0 bertsioa eta ondorengoak.

Xehetasuna:

- Ahultasun bat aurkitu da Citrix-en Application Delivery Management Agent-en (ADM). Hori baliatuz administrazio agentearen interfazerako sare sarbidea lukeen autentifikaziorik gabeko erasotzaile batek informazio konfidentziala eskura lezake. Zabaldutako informazioa erabil liteke agentetik haragoko pribilegioen eskalatzea lortzeko. Ahultasun horretarako CVE-2019-9548 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Netgear-en produktuetan

Argitalpen data: 2019/03/12

Garrantzia: Handia

Kaltetutako baliabideak:

- D3600, firmwarearen 1.0.0.75 bertsioa baino lehenagokoak
- D6000, firmwarearen 1.0.0.75 bertsioa baino lehenagokoak
- D6100, firmwarearen 1.0.0.60 bertsioa baino lehenagokoak
- D8500, firmwarearen 1.0.3.43 bertsioa baino lehenagokoak
- R6400, firmwarearen 1.0.1.44 bertsioa baino lehenagokoak
- R6700, firmwarearen 1.0.2.6 bertsioa baino lehenagokoak
- R6900, firmwarearen 1.0.2.4 bertsioa baino lehenagokoak
- R6900P, firmwarearen 1.3.1.44 bertsioa baino lehenagokoak
- R7000, firmwarearen 1.0.9.42 bertsioa baino lehenagokoak
- R7000P, firmwarearen 1.3.1.44 bertsioa baino lehenagokoak
- R7100LG, firmwarearen 1.0.0.48 bertsioa baino lehenagokoak
- R7300, firmwarearen 1.0.0.68 bertsioa baino lehenagokoak
- R7800, firmwarearen 1.0.2.62 bertsioa baino lehenagokoak
- R7900P, firmwarearen 1.4.1.30 bertsioa baino lehenagokoak
- R8000, firmwarearen 1.0.4.28 bertsioa baino lehenagokoak
- R8000P, firmwarearen 1.4.1.30 bertsioa baino lehenagokoak
- R8300, firmwarearen 1.0.2.128 bertsioa baino lehenagokoak
- R8500, firmwarearen 1.0.2.128 bertsioa baino lehenagokoak
- R8900, firmwarearen 1.0.4.26 bertsioa baino lehenagokoak
- R9000, firmwarearen 1.0.4.26 bertsioa baino lehenagokoak
- WNDR3700v4, firmwarearen 1.0.2.102 bertsioa baino lehenagokoak
- WNDR4300, firmwarearen 1.0.2.104 bertsioa baino lehenagokoak
- WNDR4300v2 eta WNDR4500v3, firmwarearen 1.0.0.58 bertsioa baino lehenagokoak
- WNR2000v5, firmwarearen 1.0.0.66 bertsioa baino lehenagokoak

Azalpena:

Ohartarazpen honek Netgear produktuei eragiten dieten 11 ahultasun jasotzen ditu eta horietatik 4 larritasun altukoak dira.

Konponbidea:

- Firmwarearen azken bertsiora eguneratzea, beraien webgunean eskuragarri.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunak balia litzake ondoko ekintzak egin ahal izateko:

- Autentifikazioaren ondoren komandoak injektatzea.
- Autentifikazioaren ondoren pilari (stack) gainezka eginaraztea.
- Cross-site scripting.
- Autentifikazioari ihes egitea.
- Bufferrari gainezka eginaraztea autentifikazioaren ondoren.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun F5en BIG-IPn

Argitalpen data: 2019/03/12

Garrantzia: Handia

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), ondoko bertsioak:
  - 14.0.0
  - 13.0.0tik 13.1.1era bitartekoak
  - 12.1.0tik 12.1.4ra bitartekoak
  - 11.6.1etik 11.6.3ra bitartekoak
  - 11.2.1etik 11.5.9ra bitartekoak
- Entreprise Manager, 3.1.1 bertsioa

Azalpena:

F5ek bere produktuei eragiten dieten hainbat ahultasunen berri eman du, horietako bat kritikotasun altukoa, bi kritikotasun ertainekoak eta hiru kritikotasun baxukoak.

Konponbidea:

- BIG-IP (LTM, AAM, AFM, Analytics, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) ondoko bertsioetara eguneratzea, ahultasunaren eta beren adarraren arabera:
  - 14.x adarraren kasuan, 14.0.0, 14.1.0 edo 14.0.0.3 bertsioetara eguneratzea
  - 13.x adarraren kasuan, 13.0.1, 13.0.0HF, 13.1.0, 13.1.0.8 edo 13.1.1.2 bertsioetara eguneratzea
  - 12.x adarraren kasuan, 12.0.0, 12.1.3.7 edo 12.1.4 bertsioetara eguneratzea
  - 11.x adarraren kasuan, 11.6.3.3 edo 11.5.9 bertsioetara eguneratzea

Xehetasuna:

- Kritikotasun altuko ahultasunaren arrazoia TMMk (Traffic Management Microkernel) duen memoriaren hondatzea da DTLS saioan ClientHello mezu zatikatuak prozesatzen dituenean. Horren ondorioz ustekabeko itxiera gerta liteke. Erasotzaile batek ahultasun hori balia lezake zerbitzuaren ukapen egoera eragiteko. Ahultasun horretarako CVE-2019-6596 identifikatzailea erreserbatu da.
- Gainerako ahultasunak larritasun ertain eta baxukoak dira, eta beraientzat ondoko identifikatzaileak erreserbatu dira: CVE-2019-6599, CVE-2019-6601, CVE-2019-6600, CVE-2019-6598, CVE-2019-6597.

Etiketak: Eguneraketa, Ahultasuna

SAPen 2019ko martxoko segurtasun eguneraketa

Argitalpen data: 2019/03/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa
- SAP HANA Extended Application Services, 1 bertsioa.
- SAP NetWeaver Java Application Server (J2EE-APPS), 7.10etik 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50era bitarteko bertsioak.
- ABAP Server (NetWeaver eta Suite/ERPn erabilia), Kernel 7.21 edo 7.22 erabiltzen duen bertsioa, ABAP Server 7.00tik 7.31ra, Kernel 7.45, 7.49 edo 7.53 erabiltzen duten bertsioak, ABAP Server 7.40tik 7.52era edo ABAP Platform.
- ABAP Server of SAP NetWeaver eta ABAP Platform, honako bertsioak: KRNL32NUC 7.21, KRNL32NUC 7.21EXT, KRNL32NUC 7.22, KRNL32NUC 7.22EXT, KRNL32UC 7.21, KRNL32UC 7.21EXT, KRNL32UC 7.22, KRNL32UC 7.22EXT, KRNL64NUC 7.21, KRNL64NUC 7.21EXT, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, KRNL64NUC 7.49, KRNL64NUC 7.74, KRNL64UC 7.21, KRNL64UC 7.21EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.49, KRNL64UC 7.73, KRNL64UC 7.74, KRNL64UC 8.04, KERNEL 7.21, KERNEL 7.45, KERNEL 7.49, KERNEL 7.53, KERNEL 7.73, KERNEL 7.74, KERNEL 7.75 eta KERNEL 8.04.
- ABAP Platform (SLD Registration), honako bertsioak: KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT; KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT; KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49; KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49. 7.73; KERNEL 7.21etik 7.22ra bitartekoak, 7.45, 7.49, 7.53, 7.73 eta 7.75.
- SAP Mobile Platform SDK, SDK 3.1 SP03 PL02 eta SDK 3.1 SP04 baino lehenagoko bertsioak.
- SAP BusinessObjects Business Intelligence Platform (BI Workspace), 4.10 eta 4.20 bertsioak.
- SAP BusinessObjects Business Intelligence Platform (CMC Module), 4.10, 4.20 eta 4.30 bertsioak.
- SAP Plant Connectivity, 15.1 eta 15.2 bertsioak.
- SAP Enterprise Financial Services, SAPSCORE 1.13, 1.14 eta 1.15 eta S4CORE 1.01, 1.02 eta 1.03 bertsioak.
- EA-FINSERV 1.10, 2.0, 5.0, 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0 eta Bank/CFM 4.63_20.
- FSAPPL, 5 bertsioa.
- S4FPSL, 1 bertsioa.
- Banking services SAPetik, 9.0 bertsioa.

Azalpena:

SAPek hainbat produkturi buruzko segurtasun eguneraketa batzuk argitaratu ditu bere hileroko komunikatuan.

Konponbidea:

- SAPen laguntza ataria bisitatu eta fabrikatzaileak adierazten duen moduan beharrezkoak diren eguneraketa edo partxeak instalatzea.

Xehetasuna:

SAPek segurtasun partxeei buruz argitaratzen duen hileroko komunikatuan 9 segurtasun ohar eta 3 eguneraketa eman ditu ezagutzera. Horietatik 1 larritasun kritikokoa da, 2 larritasun altukoak eta beste 9 larritasun ertainekoak.

Argitaratutako ahultasun motak ondokoak dira:

- Baimenaren egiaztapen gabeziako 3 ahultasun.
- XSS (Cross-Site Scripting) erako 2 ahultasun.
- Zerbitzuaren ukazioko ahultasun bat.
- XML External entity erako 4 ahultasun.
- Beste era batzuetako 2 ahultasun.

Kritikotzat kalifikatutako segurtasun oharra honi buruzkoa da:

- SAP Business Client-ek duen ahultasun bat baliatuz, erasotzaile batek bereziki diseinatutako kodea injekta lezake memorian. Horrela zerbitzuaren ukapena edo kodearen urruneko exekuzioa eragingo luke.

Etiketak: Eguneraketa, SAP, Ahultasuna

Joomla! 3.9.4ren segurtasun eguneraketa

Argitalpen data: 2019/03/13

Garrantzia: Handia

Kaltetutako baliabideak:

- Joomla! CMS, 3.0.0tik 3.9.3ra bitarteko bertsioak

Azalpena:

Joomla!-k bertsio berri bat argitaratu du, nukleoak dituen lau ahultasun konpontzen dituena, bat kritikotasun altukoa eta hiru kritikotasun txikikoak. Guztiak dira XSS (Cross-site scripting) erakoak.

Konponbidea:

- 3.9.4 bertsiora eguneratu.

Xehetasuna:

- Kritikotasun altuko ahultasunaren arrazoia lagineko pluginetan ACLk (Access Control List) duen egiaztatze eza da. Hori baliatuz erasotzaile batek baimenik gabeko sarbidea lor lezake. Ahultasun horretarako CVE-2019-9713 identifikatzailea erabili da.
- Gainerako ahultasunetarako honako identifikatzaileak esleitu dira: CVE-2019-9714, CVE-2019-9711 eta CVE-2019-9714.

Etiketak: Eguneraketa, CMS, Ahultasuna

Pribilegioen igoera IBM DB2n

Argitalpen data: 2019/03/13

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM DB2, V9.7, V10.1, V10.5 eta V11.1 bertsioak, plataforma guztietan.

Azalpena:

IBMk bere IBM DB2 produktuek duten ahultasun baten berri eman du. Hori baliatuz erasotzaile batek pribilegioen eskalatzea lor lezake, pribilegio baxuko erabiltzaile lokal batetik *root* pribilegioak lituzkeen erabiltzaile bateraino.

Konponbidea:

Dagokion partxea aplikatzea, bertsioaren eta plataformaren arabera.

- DB2 V11.1ren kasuan, V11.1.4.4 iFix001 partxea deskargatzeko eskuragarri dago IBM Fix Central-en.
- Ahultasuna duen beste edozein bertsioren kasuan, plataforma bakoitzerako behin-behineko partxe bat deskarga daiteke , IBM Fix Central-etik "Erreferentziak" atalean aipatutako buletinaren arabera.

Xehetasuna:

- Linux, UNIX eta Windowserako IBM DB2k (DB2 Connect Server-ek barne) fidagarria ez den bide batetik liburutegiak deskargatzen ditu. Erasotzaile batek hori balia lezake asmo gaiztoko liburutegi bat deskargatzeko eta pribilegio gutxiko erabiltzaile bati pribilegioak eskalatzea ahalbidetu liezaioke *root* mailaraino. Ahultasun horretarako CVE-2019-4094 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Netgear-en produktuetan

Argitalpen data: 2019/03/13

Garrantzia: Handia

Kaltetutako baliabideak:

- D6220, firmwarearen 1.0.0.46 bertsioa baino lehenagokoa dutenak
- D6400, firmwarearen 1.0.0.80 bertsioa baino lehenagokoa dutenak
- D7000v2, firmwarearen 1.0.0.51 bertsioa baino lehenagokoa dutenak

- D8500, firmwarearen 1.0.3.42 bertsioa baino lehenagokoa dutenak
- DGN2200, firmwarearen 1.0.0.58 bertsioa baino lehenagokoa dutenak
- DGN2200B, firmwarearen 1.0.0.58 bertsioa baino lehenagokoa dutenak
- DGN2200v1, firmwarearen 1.0.0.58 bertsioa baino lehenagokoa dutenak
- EX3700, firmwarearen 1.0.0.70 bertsioa baino lehenagokoa dutenak
- EX3800, firmwarearen 1.0.0.70 bertsioa baino lehenagokoa dutenak
- EX6000, firmwarearen 1.0.0.30 bertsioa baino lehenagokoa dutenak
- EX6100, firmwarearen 1.0.2.22 bertsioa baino lehenagokoa dutenak
- EX6120, firmwarearen 1.0.0.40 bertsioa baino lehenagokoa dutenak
- EX6130, firmwarearen 1.0.0.22 bertsioa baino lehenagokoa dutenak
- EX6150, firmwarearen 1.0.0.42 bertsioa baino lehenagokoa dutenak
- EX6200, firmwarearen 1.0.3.88 bertsioa baino lehenagokoa dutenak
- EX7000, firmwarearen 1.0.0.66 bertsioa baino lehenagokoa dutenak
- EX7500, firmwarearen 1.0.0.46 bertsioa baino lehenagokoa dutenak
- JNDR3000, firmwarearen 1.0.0.24 bertsioa baino lehenagokoa dutenak
- R6250, firmwarearen 1.0.4.26 bertsioa baino lehenagokoa dutenak
- R6300v2, firmwarearen 1.0.4.28 bertsioa baino lehenagokoa dutenak
- R6400, firmwarearen 1.0.1.42 bertsioa baino lehenagokoa dutenak
- R6400v2, firmwarearen 1.0.2.56 bertsioa baino lehenagokoa dutenak
- R6700, firmwarearen 1.0.1.46 bertsioa baino lehenagokoa dutenak
- R6900, firmwarearen 1.0.1.46 bertsioa baino lehenagokoa dutenak
- R6900P, firmwarearen 1.3.2.34 bertsioa baino lehenagokoa dutenak
- R7000, firmwarearen 1.0.9.32 bertsioa baino lehenagokoa dutenak
- R7000P, firmwarearen 1.3.2.34 bertsioa baino lehenagokoa dutenak
- R7100LG, firmwarearen 1.0.0.46 bertsioa baino lehenagokoa dutenak
- R7300DST, firmwarearen 1.0.0.68 bertsioa baino lehenagokoa dutenak
- R7900, firmwarearen 1.0.2.16 bertsioa baino lehenagokoa dutenak
- R7900P, firmwarearen 1.4.0.10 bertsioa baino lehenagokoa dutenak
- R8000, firmwarearen 1.0.4.18 bertsioa baino lehenagokoa dutenak
- R8000P, firmwarearen 1.4.0.10 bertsioa baino lehenagokoa dutenak
- R8300, firmwarearen 1.0.2.122 bertsioa baino lehenagokoa dutenak
- R8500, firmwarearen 1.0.2.122 bertsioa baino lehenagokoa dutenak
- RBW30, firmwarearen 2.1.4.16 bertsioa baino lehenagokoa dutenak
- WN2500RPv2, firmwarearen 1.0.1.54 bertsioa baino lehenagokoa dutenak
- WN3100RP, firmwarearen 1.0.0.20 bertsioa baino lehenagokoa dutenak
- WNDR3400v3, firmwarearen 1.0.1.22 bertsioa baino lehenagokoa dutenak
- WNDR4500v2, firmwarearen 1.0.0.72 bertsioa baino lehenagokoa dutenak
- WNR3500Lv2, firmwarearen 1.2.0.54 bertsioa baino lehenagokoa dutenak

Azalpena:

Netgear-ek 4 segurtasun ohartarazpen argitaratu ditu, 2 larritasun altukoak, 1 ertainekoa eta 1 baxukoa.

Konponbidea:

- Firmwarearen azken bertsiora eguneratzea, beraien webgunean eskuragarri.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunak balia litzake ondoko ekintzak egin ahal izateko:

- pilaren gainezkatzea autentifikazioaren aurretik,
- cross-site scripting (XSS) islatua,
- bufferraren gainezkatzea autentifikazioaren ondoren,
- pilaren gainezkatzea autentifikazioaren ondoren.

Etiketak: Eguneraketa,

Hainbat ahultasun Intel-en produktuetan

Argitalpen data: 2019/03/13

Garrantzia: Handia

Kaltetutako baliabideak:

- Intel® CSME, 11.8.60, 11.11.60, 11.22.60 edo 12.0.20 bertsioa baino lehenagokoak
- Intel® Server Platform Services, 4.00.04.383 eta 4.01.02.174 bertsioa baino lehenagokoak
- Intel® Trusted Execution Engine, 3.1.60 edo 4.0.10 bertsioa baino lehenagokoak
- Widowserako Intel® Graphics Driver, bertsio hauek baino lehenagokoak: 10.18.x.5059 (15.33.x.5059 modura ere ezaguna), 10.18.x.5057 (15.36.x.5057 modura ere ezaguna), 20.19.x.5063 (15.40.x.5063 modura ere ezaguna) 21.20.x.5064 (15.45.x.5064 modura ere ezaguna) eta 24.20.100.6373
- Plataformen ondorengo belaunaldietan dagoen firmwarea:
  - 8th Generation Intel(R) Core™ Processor
  - 7th Generation Intel(R) Core™ Processor
  - Intel(R) Pentium(R) Silver J5005 Processor
  - Intel(R) Pentium(R) Silver N5000 Processor
  - Intel(R) Celeron(R) J4105 Processor
  - Intel(R) Celeron(R) J4005 Processor
  - Intel® Celeron(R) N4100 Processor
  - Intel(R) Celeron® N4000 Processor
  - Intel(R) Server Board
  - Intel(R) Server System
  - Intel(R) Compute Module
- Intel® Matrix Storage Manager, 8.9.0.1023 eta lehenagoko bertsioak..
- Intel® Accelerated Storage Manager in RSTe, v5.5 eta lehenagoko bertsioak.
- Intel® SGX SDK
  - Linuxerako, 2.2 baino lehenagoko bertsioak2
  - Windowserako, 2.1 baino lehenagoko bertsioak
- Intel® USB 3.0 Creator Utility, bertsio guztiak.

Azalpena:

Intelek 7 ohartarazpen argitaratu ditu produktuen bere segurtasun zentroan, guztira 40 ahultasunen berri emanez. Horietako 11 larritasun altukoak dira eta gainerakoak larritasun ertain edo txikikoak.

Konponbidea:

- Kaltetutako produktua azken bertsiora eguneratu, euren deskargen zentroan eskuragarri.

Xehetasuna:

Larritasun altuko ahultasunak honakoak dira:

- Intel® CSME azpisistemak duen sarreraren baliozkotze ez-nahikoa baliatuz, erabiltzaile pribilegiatu batek kode arbitrarioa exekuta lezake sarbide lokaletik. Ahultasun horretarako CVE-2018-12190 identifikatzailea erreserbatu da.
- Intel(R) CSMEko HECI azpisistemak duen bufferraren gainezkatzea baliatuz, autentifikaziorik gabeko erabiltzaile batek kode arbitrarioa exekuta lezake sarbide fisikotik. Ahultasun horretarako CVE-2018-12208 identifikatzailea erreserbatu da.
- Intel(R) Capability Licensing Servicek duen sarbidearen kontrol ez-nahikoa baliatuz, pribilegiorik gabeko erabiltzaile batek pribilegioen eskalatzea egin lezake sarbide fisikotik. Ahultasun horretarako CVE-2018-12200 identifikatzailea erreserbatu da.
- Intel(R) Active Management Technology-k (Intel(R) AMT) duen sarreraren baliozkotze ez-nahikoa baliatuz, autentifikaziorik gabeko erabiltzaile batek zerbitzuaren ukapena eragin lezake sareko sarbidearen bidez. Ahultasun horretarako CVE-2018-12187 identifikatzailea erreserbatu da.
- Intel(R) CSMEko Intel(R) AMTk duen sarreraren baliozkotze ez-nahikoa baliatuz, autentifikaziorik gabeko erabiltzaile batek kode arbitrarioa exekuta lezake sarbide lokaletik. Ahultasun horretarako CVE-2018-12185 identifikatzailea erreserbatu da.
- Windowserako Intel(R) Graphics Driver-eko Kernel Mode Driver-ek duen memoriaren hondatzea baliatuz, erabiltzaile pribilegiatu batek kode arbitrarioa exekuta lezake sarbide lokaletik. Ahultasun horretarako CVE-2018-12214 identifikatzailea erreserbatu da.
- Windowserako Intel(R) Graphics Driver-eko Kernel Mode Driver-ek duen sarreraren baliozkotze ez-nahikoa baliatuz, erabiltzaile pribilegiatu batek kode arbitrarioa exekuta lezake sarbide lokaletik. Ahultasun horretarako CVE-2018-12216 identifikatzailea erreserbatu da.
- Platform Sample/Silicon Reference firmware Intel(R) Server Board, Intel(R) Server System eta Intel(R) Compute Module-k duten pribilegioen eskalatze erako ahultasun bat baliatuz, erabiltzaile pribilegiatu batek kode arbitrarioa exekuta lezake sarbide lokaletik. Ahultasun horretarako CVE-2018-12204 identifikatzailea erreserbatu da.
- 8th Generation Intel(R) CoreTM Processor eta 7th Generation Intel(R) CoreTM Processor-erako Platform Sample/ Silicon Reference firmwareak duen pribilegioen eskalatze erako ahultasun bat baliatuz, autentifikaziorik gabeko erabiltzaile batek kode arbitrarioa exekuta lezake sarbide fisikotik. Ahultasun horretarako CVE-2018-12205 identifikatzailea erreserbatu da.
- Intel(R) Matrix Storage Manager-ek duen baimen okerren ahultasun bat baliatuz, erabiltzaile autentifikatu batek pribilegioen eskalatze bat egin lezake sarbide lokaletik. Ahultasun horretarako CVE-2019-0121 identifikatzailea erreserbatu da.
- Intel(R) Accelerated Storage Manager in RSTe-ren instalatzaileak duen baimen okerren ahultasun bat baliatuz, autentifikaziorik gabeko erabiltzaile batek pribilegioen eskalatze bat egin lezake sarbide lokaletik. Ahultasun horretarako CVE-2019-0135 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Microsoften 2019ko martxoko segurtasun buletina

Argitalpen data: 2019/03/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Adobe Flash Player
- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office y Microsoft Office SharePoint
- ChakraCore
- Team Foundation Server
- Skype for Business
- Visual Studio
- NuGet

Azalpena:

Segurtasun eguneraketei buruzko Microsoften hileroko argitalpenean 63 ahultasun jaso dira oraingoan, 18 kritiko gisa sailkatu dira eta 45 garrantzitsu gisa.

Konponbidea:

- Dagozkien segurtasun eguneraketak instalatzea. Eguneraketa horien beraien instalazioaren informazio orrian hori egiteko metodo ezberdinei buruzko argibideak daude.

Xehetasuna:

Argitaratutako ahultasun motak ondokoak dira:

- Pribilegioen eskalatzea.
- Zerbitzuaren ukapena.
- Informazioa ezagutaraztea.
- Manipulazioa.
- Kodearen urruneko exekuzioa..
- Ordezpena.
- Segurtasunari ihes egitea.

Etiketak: Eguneraketa, Microsoft, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/03/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco Common Services Platform Collector (CSPC), 2.7.2tik 2.7.4.5ra bitarteko bertsioak, eta 2.8.1.2 baino lehenagoko 2.8.x bertsio guztiak
- Cisco Small Business SPA514G IP Phone, firmwarearen 7.6.2SR2 edo lehenagoko bertsioa exekutatzen ari bada.

Azalpena:

Bi ahultasun aurkitu dira, bat larritasun kritikokoa eta bestea altukoa, Cisco Common Services Platform Collector (CSPC) eta Cisco Small Business-en, hurrenez hurren.

Konponbidea:

- Cisco CSPC, software zentrotik deskargatzea:
  - 2.7.x bertsioen kasuan, 2.7.4.6 bertsiora eguneratzea
  - 2.8.x bertsioen kasuan, 2.8.1.2 bertsiora eguneratzea
- Cisco Small Business SPA514G IP Phoneren kasuan ez da konponbiderik argitaratu eta ez da argitaratuko etorkizunean ere, produktua end-of-life prozesuan sartuta baitago eta laster zerbitzurik ez baitu izango.

Xehetasuna:

- Cisco CSPCk duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek kaltetutako gailura sarbidea lor lezake, pasahitz lehenetsia eta estatikoa duen kontu bat erabiliz. Kontu honek ez du administratzaile konturik. Ahultasun horretarako CVE-2019-1723 identifikatzailea erabili da.
- Cisco Small Business SPA514G IP Phone-n Session Initiation Protocol-en (SIP) prozesatzearen inplementazioak duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek eragin lezake kaltetutako gailuak ez erantzutea, eta horren ondorioz zerbitzuaren ukapen egoera (DoS) gertatuko litzateke. Ahultasun horretarako CVE-2018-0389 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Pribilegioak eskalatzearen erako ahultasuna IBMren Db2-n

Argitalpen data: 2019/03/15

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM Db2, plataforma guztietan, ondoko bertsioak:
  - 9.7
  - 10.1
  - 10.5
  - 11.1

Azalpena:

IBMren Db2-k duen kritikotasun altuko ahultasun bat baliatuz, erasotzaile batek pribilegioak eskalatzea lor lezake root baimenekin.

Konponbidea:

- IBMk ahultasuna arintzen duten hainbat eguneraketa eta segurtasun partxe argitaratu ditu, bertsioaren eta kaltetutako produktuaren arabera.
  - 9.7 bertsioa, 9.7 FP11 bertsiora eguneratu.
  - 10.1 bertsioa, 10.1 FP6 bertsiora eguneratu.
  - 10.5 bertsioa, 10.5 FP10 bertsiora eguneratu.
  - 11.1 bertsiora, 11.1.4.4 iFix001 partxea apliatu.

Xehetasuna:

- Ahultasunaren arrazoia da bitarrek liburutegi partekatuak bide ez fidagarri batetik kargatzen zutela. Hori baliatuz, pribilegio baxuko erabiltzaile batek sistemara sarbidea lor lezake root pribilegioekin. Erasotzaile batek asmo gaiztoko liburutegi partekatu bat karga lezake sisteman pribilegioen eskalatzea egiteko. Ahultasun horretarako CVE-2019-4094 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Informazioaren zabalkundean HPEren NonStop SafeGuard-en

Argitalpen data: 2019/03/15

Garrantzia: Handia

Kaltetutako baliabideak:

- SAFEGUARD: T9750L01^AID edo T9750H05^AIH baino lehenagoko bertsio guztiak, eta ondorenekoak PASSWORD-PROMPT konfigurazio atributua BLIND-en konfiguratuta ez dagoenean.
- STDSEC-STANDARD SECURITY PROD: T6533L01^ADU edo T6533H05^ADW baino lehenagoko bertsio guztiak, eta ondorenekoak PASSWORD-PROMPT konfigurazio atributua BLIND-en konfiguratuta ez dagoenean.

Azalpena:

HPEk bere NonStop SafeGuard produktuak duen ahultasun bat argitaratu du. Hori baliatuz erasotzaile batek kredentzialen zabalkunde lokala egitea lor lezake.

Konponbidea:

SPR egokiak instalatzea bertsio bakoitzaren arabera:

- L-series:
  - T9750L01^AID (SAFEGUARD), dagoeneko eskuragarri
  - T6533L01^ADU (STDSEC-STANDARD SECURITY PROD), dagoeneko eskuragarri
- J-series:
  - T9750H05^AIH (SAFEGUARD) - hurrengo J-series RVU-n egongo da eskuragarri
  - T6533H05^ADW (STDSEC-STANDARD SECURITY PROD) - hurrengo J-series RVU-n egongo da eskuragarri

Xehetasuna:

- NonStop Safeguard eta NonStop Standard Security softwarearen komando batzuek erabiltzaile izena eta pasahitza komandoen lerroko parametro modura pasatuak izan daitezen eskatzen dute, eta horrek eragin dezake kredentzialen zabalkunde lokala gertatzea. Ahultasun horretarako CVE-2018-7119 identifikatzailea erreserbatu da.

Etiketak: HP, Ahultasuna

Hainbat ahultasun VMware-n

Argitalpen data: 2019/03/18

Garrantzia: Handia

Kaltetutako baliabideak:

- VMware Workstation Pro / Player (Workstation), adar hauetan:
  - 15.X Windows sistemetan.
  - 14.X Windows sistemetan.
- VMware Horizon, adar hauetan:
  - Horizon 7 (CR) 7.X
  - Horizon 7 (ESB) 7.5.X
  - Horizon 6 6.X

Azalpena:

VMwarek hiru ahultasun aurkitu ditu hainbat produktutan. Horietatik bi kritikotasun altukoak dira eta bestea kritikotasun ertainekoa.

Konponbidea:

VMwarek ahultasun horiek arintzen dituzten hainbat eguneraketa argitaratu ditu, kaltetutako produktuaren eta adarraren arabera:

- VMware Workstation Pro / Player (Workstation):
  - 15.X Windows sistemetan, 15.0.3 eguneraketa aplikatu.
  - 14.X Windows sistemetan, 14.1.6 eguneraketa aplikatu.
- VMware Horizon:
  - Horizon 7 (CR) 7.X, 7.8 KB67424 partxea aplikatu.
  - Horizon 7 (ESB) 7.5.X, 7.5.2 KB67401 partxea aplikatu.
  - Horizon 6 6.X, 6.2.8 KB67401 partxea aplikatu.

Xehetasuna:

- Workstation-ek bideen kudeaketa oker batengatik duen ahultasun bat baliatuz, erasotzaile batek VMX exekutagarrira sarbidea lor lezake, eta horren ondorioz sistemaren bahiketa eta erabiltzailearen pribilegioen eskalatzea gerta litezke. Ahultasun horretarako CVE-2018-5511 identifikatzailea erabili da.
- Workstation-ek COM klaseen kudeaketa oker batengatik duen ahultasun bat baliatuz, erasotzaile batek VMX prozesua bahitu lezake COM klaseen bidez, eta horren ondorioz pribilegioen eskalatzea gerta liteke. Ahultasun horretarako CVE-2019-5512 identifikatzailea erreserbatu da.
- Kritikotasun ertaineko ahultasunerako CVE-2019-5513 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Urruneko backend HTTPren baliozkotze ez-nahikoa PowerDNS-n

Argitalpen data: 2019/03/19

Garrantzia: Handia

Kaltetutako baliabideak:

- PowerDNS Authoritative, 4.1.6 eta lehenagoko bertsioak.

Azalpena:

Kritikotasun altuko ahultasun bat baliatuz, urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake, informazioa hedatu edo

edukia faltsutu.

Konponbidea:

- 4.1.7 edo 4.0.7 bertsioetara eguneratzea.

Xehetasuna:

- PowerDNS Authoritative Server-en urruneko backend HTTP-k *RESTful* moduan erabiltzen denean daukan akats bat baliatuz, urruneko erasotzaile batek zerbitzuaren ukapen egoera, edukiaren faltsutzea edo informazioaren zabalkundea eragin lezake, asmo gaiztoko DNS eskari bat sortuz. Ahultasun horretarako CVE-2019-3871 identifikatzailea erabili da.

Etiketak: Eguneraketa, DNS, Ahultasuna

Hainbat ahultasun Moodle-n

Argitalpen data: 2019/03/19

Garrantzia: Handia

Kaltetutako baliabideak:

Ondoko bertsioak izan dira kaltetuak, ahultasunen arabera:

- MSA-19-0004 eta MSA-19-0007: 3.6tik 3.6.2ra bitartekoak, 3.5etik 3.5.4ra bitartekoak, 3.4tik 3.4.7ra bitartekoak, 3.1etik 3.1.16ra bitartekoak eta zerbitzurik gabeko lehenagoko bertsioak.
- MSA-19-0005: 3.6tik 3.6.2ra bitartekoak, 3.5etik 3.5.4ra bitartekoak eta 3.4tik 3.4.7ra bitartekoak
- MSA-19-0006: 3.6tik 3.6.2ra bitartekoak, 3.5etik 3.5.4ra bitartekoak, 3.4tik 3.4.7ra bitartekoak, eta zerbitzurik gabeko lehenagoko bertsioak.
- MSA-19-0008: 3.6tik 3.6.2ra bitartekoak eta 3.5etik 3.5.4ra bitartekoak.
- MSA-19-0009: 3.6tik 3.6.2ra bitartekoak

Azalpena:

Moodle plataforman 6 ahultasun aurkitu dira, hiru kritikotasun altukoak eta beste hiru kritikotasun baxukoak.

Konponbidea:

Erabiltzaileen eskura jarri dira ondoko eguneraketak, ahultasun bakoitzaren arabera:

- MSA-19-0004 eta MSA-19-0007: 3.6.3, 3.5.5, 3.4.8 eta 3.1.17.
- MSA-19-0005 eta MSA-19-0006: 3.6.3, 3.5.5 eta 3.4.8.
- MSA-19-0008: 3.6.3 eta 3.5.5
- MSA-19-0009: 3.6.3

Xehetasuna:

Kritikotasun altuko ahultasunak ondokoak dira:

- *Login as other users* (administratzaile modura) gaitasuna duten erabiltzaileek beste erabiltzaile batzuen *dashboard*-etara sar daitezke, baina erabiltzaile horiek beren *dashboard*-era gehitu ahal izan zuten JavaScript-ak ez zuen ihes egiten bere izenean saioa hasten zuen erabiltzaileak ikusten zuenean. Ahultasun horretarako CVE-2019-3847 identifikatzailea erreserbatu da.
- Egutegiko ekitaldiak editatzeko azaleratzen den leiho modalean ekitaldien informazioa kargatu aurretik baimenak ez ziren zuzenki egiaztatu. Hortaz, saioa hasi duten gonbidapenik gabeko erabiltzaileek egutegiko ekitaldi baimenik gabeak ikus ditzakete. (Oharra: Irakurketa hutseko sarbidea zen, erabiltzaileek ezin zuten ekitaldirik editatu). Ahultasun horretarako CVE-2019-3848 identifikatzailea erreserbatu da.
- Erabiltzaileek LTIren bidez (*Learning Tools Interoperability*) sarbidea lortzen den ikastaroen edo edukien barnean dagokiena baino rol altuagoa eman diezaiokete beren buruari, LTIren editorearen webgunerako eskaera aldatuz. Ahultasun horretarako CVE-2019-3849 identifikatzailea erreserbatu da.

Kritikotasun baxuko gainerako ahultasunetarako honako identifikatzaileak esleitu dira: CVE-2019-3850, CVE-2019-3851 eta CVE-2019-3852.

Etiketak: Eguneraketa, CMS, Ahultasuna

Cross-Site Scripting erako ahultasuna Drupal-en core-an

Argitalpen data: 2019/03/21

Garrantzia: Ertaina

Kaltetutako baliabideak:

- 8.6.13 baino lehenagoko 8.6.x bertsioak
- 8.5.14 baino lehenagoko 8.5.x bertsioak
- 7.65 baino lehenagoko 7.x bertsioak

Azalpena:

Cross-Site Scripting (XSS) erako ahultasuna aurkitu da Drupal-en *core*-an.

Konponbidea:

- Drupal 8.6 bertsioaren kasuan, 8.6.13 bertsiora eguneratzea.
- Drupal 8.5 bertsioaren edo lehenagokoen kasuan, 8.5.14 bertsiora eguneratzea.
- Drupal 7 bertsioaren kasuan, 7.65 bertsiora eguneratzea.

8.5.x baino lehenagoko Drupal 8 bertsioak end-of-life fasean daude eta, ondorioz, ez dute segurtasun eguneraketarik izaten.

Xehetasuna:

- Egoera batzuetan fitxategien modulu/azpisistemak ahalbidetzen du asmo gaiztoko erabiltzaile batek *Cross-Site Scripting* (XSS) erako ahultasun bat eragin dezakeen fitxategi bat kargatzea.

Etiketak: CMS, Ahultasuna

Hainbat ahultasun Cisco-ren IP telefonoetan

Argitalpena data: 2019/03/21

Garrantzia: Handia

Kaltetutako baliabideak:

Ciscoren IP telefonoak, SIP softwarea exekutatzen dutenak ondorengo bertsioak baino lehenagokoetan:

- Unified IP Conference Phone 8831erako 10.3(1)SR5
- Wireless IP Phone 8821 eta 8821-EXerako 11.0(4)SR3 eta 11.0(5)
- IP Conference Phone 8832, IP Phone 8800 eta IP Phone 7800 serieetarako 12.5(1)SR1

Azalpena:

Ciscok kritikotasun altuko 5 ahultasun aurkitu ditu, bere IP telefono batzuei eragiten dietenak.

Konponbidea

- Ciscok bere erabiltzaileen eskura jarri ditu ahultasun horiek arintzen dituzten hainbat eguneraketa, bertsioaren eta kaltetutako produktuaren arabera. Eguneraketa Ciscoren software zentrotik deskarga daiteke.

Xehetasuna:

Aurkitutako ahultasunak baliatuz autentifikaziorik gabeko urruneko erasotzaile batek ondokoa egin lezake:

- Fitxategien baimenik gabeko aldaketa.
- Zerbitzuaren ukapen egoera (Dos) eragin.
- Autentifikazio egiaztapenak saihestu.
- Zerbitzu kritikoetara sarbidea lortu.
- Kodearen exekuzio arbitrarioa.
- Pribilegioak lortzea.

Ahultasun horietarako CVE-2019-1764, CVE-2019-1716, CVE-2019-1763, CVE-2019-1766 etaCVE-2019-1765 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Ahultasuna IBMren API Connect-en

Argitalpen data: 2019/03/22

Garantzia: Handia

Kaltetutako baliabideak:

- IBM API Connect, 2018.1 bertsiotik 2018.4.1.2ra bitartekoak

Azalpena:

IBMk kritikotasun altuko ahultasun bat aurkitu du IBM API Connect 2018-n.

Konponbidea:

- IBM Connect 2018.4.1.3 bertsiora eguneratzea

Xehetasuna:

- Autentifikaziorik gabeko erasotzaile batek, IBM Connect-en APIa baliatuz, erabiltzaile erregistratuen sarbide IDak eskura litzake. Ahultasun horretarako CVE-2019-4052 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun F5en produktuetan

Argitalpen data: 2019/03/22

Garrantzia: Handia

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), ondoko bertsioak:
-

    - 14.0.0
    - 13.0.0tik 13.1.1era bitartekoak
    - 12.0.x
    - 12.1.0tik 12.1.3ra bitartekoak
    - 11.2.1etik 11.6.3ra bitartekoak
- BIG-IP (ASM), ondoko bertsioak:
-
    - 14.0.0tik 14.0.0.2ra bitartekoak
    - 13.0.0tik 13.1.1.3ra bitartekoak
    - 12.1.0tik 12.1.3ra bitartekoak
    - 11.6.1etik 11.6.3ra eta 11.5.1etik 11.5.8ra bitartekoak

Azalpena:

Hainbat ahultasun aurkitu dira F5en hainbat produktutan, 3 kritikotasun altukoak, 3 ertainekoak eta 1 baxukoa. Ahultasun horiek hainbat egoera eragin litzakete: zerbitzuaren urruneko etena, sendotasunik gabeko HTTP erantzuna, trafikoaren prozesamendua gelditzea, cross-site scripting (XSS) edo memoriaren kontsumo gehiegizkoa.

Konponbidea:

- F5ek erabiltzaileen eskura jarri ditu ahultasun horiek konpontzeko hainbat eguneraketa: Partxeak beren softwarearen deskarga zentroan aurki daitezke.

Xehetasuna:

Kritikotasun altuko ahultasunak ondokoak dira:

- IP helbide propio batera edo FastL4 zerbitzari birtual batera bidaltzen diren gaizki sortutako TCP paketeak zerbitzuaren eten bat eragin dezakete. Arazo honek datuen mailako zerbitzari birtualei eta IP beraiei eragiten die. Ahultasun horretarako CVE-2019-6603 identifikatzailea erreserbatu da.
- Login orriaren konfigurazio utilitateak sendotasunik gabeko HTTP erantzun bat itzultzen du eskaera aldatuak prozesatzen direnean. Horrek sisteman ahultasunak baliatzea bilatzen ari den erasotzaile bati lagundu diezaioke. Ahultasun horretarako CVE-2019-6602 identifikatzailea erreserbatu da.
- Baldintza batzuetan, lehenetsi gabeko 2. geruzako birbidalketa konfigurazioak erabiltzen dituzten HSB (High-Speed Bridge) bat duten hardware sistemek HSBaren blokeoa izan dezakete. BIG-IP sistemak prozesamendu trafikoa eteten du, eta horrek azkenean akatsezko kommutazio batera eramaten du taldean eskuragarritasun altua duen beste host batera. Ahultasun horretarako CVE-2019-6604 identifikatzailea erreserbatu da.

Gainerako ahultasunak kritikotasun ertain eta baxukoak dira eta beraientzat ondoko identifikatzaileak erreserbatu dira: CVE-2019-6607, CVE-2019-6605, CVE-2019-6606 eta CVE-2019-6608.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun PuTTYn

Argitalpen data: 2019/03/25

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- 0.70 eta lehenagoko bertsioak

Azalpena:

PuTTYk hainbat ahultasunen berri eman du, horietatik 3 larritasun kritikokoak.

Konponbidea:

- 0.71 bertsiora eguneratzea.

Xehetasuna:

Larritasun kritikoko ahultasunak honakoak dira:

- Unix PuTTYk *select*(2) erabiltzen du Unix fitxategien deskriptoreak ikusteko, mugarik gabeko *fd_set* motako aldagai bat baitute. 1024ko luzerako edo hori baino luzeagoko fitxategi batekin aurkituko balitz *fd_se*t-en, monitorea ez litzateke gai izango fitxategi hori monitorizatzeko, eta bufferraren gainezkatzea gertatuko litzateke. Ahultasun horretarako CVE-2019-9895 identifikatzailea erabili da.
- Erabiltzaile batek PuTTYren interfaze grafikoaren tresnen markoan online laguntza exekutatzen duenean, softwarea saiatzen da bere laguntza fitxategia bilatzen bere exekutagarriarekin batera. Portaera horrek ahalbidetuko luke, hain zuzen ere, erasotzaile batek biktima engainatzea, bezeroan asmo gaiztoko kodea exekuta dezan CHM fitxategiaren bahiketaren bidez. Ahultasun horretarako CVE-2019-9896 identifikatzailea erabili da.
- PuTTYk zenbaki kriptografiko erdi-ausazkoak sortzeko duen moduan akatsa dago, eta batzuetan ematen du birritan erabiltzen duela zenbaki erdi-ausazkoen multzo berdina. Ahultasun horretarako CVE-2019-9898 identifikatzailea erabili da.

Gainerako ahultasunak honakoak dira:

- Kodearen exekuzioa CHM hijacking bidez.
- Integer Overflow erako ahultasuna. Ahultasun horretarako CVE-2019-9894 identifikatzailea erabili da.
- Zerbitzuaren ukapena. Ahultasun horretarako CVE-2019-9897 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Zerbitzuaren ukapen erako ahultasuna Apache Tomcat-en

Argitalpen data: 2019/03/26

Garrantzia: Handia

Kaltetutako baliabideak:

- Apache Tomcat®, honako bertsioak:
  - 8.5.0tik 8.5.37ra bitartekoak
  - 9.0.0.M1etik 9.0.14ra bitartekoak

Azalpena:

Red Hat-eko Michal Karm Babacek-ek zerbitzuaren ukapen egoera eragiten duen ahultasun bat aurkitu du.

Konponbidea:

- 8.5.38 edo goragoko bertsiora eguneratzea.
- 9.0.16 edo goragoko bertsiora eguneratzea.

Xehetasuna:

- HTTP/2ren inplementazioak konfigurazio panel (SETTINGS) kopuru gehiegizko baten hurrenez hurreneko irekiera ahalbidetzen du, eta bezeroei ahalbidetzen die horiek zabalik izatea eskaera/erantzuneko datuak irakurri/idatzi gabe. *Servlet*-en E/Sren blokeatze APIa erabiltzen duten eskaeretarako zabalik mantentzean, bezeroek eragin dezakete zerbitzariaren aldean exekutatzen ari diren azpi-prozesuak blokeatzea, azpi-prozesuen agortze eta zerbitzuaren ukapen egoera (DoS) gertatuz. Ahultasun horretarako CVE-2019-0199 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Apache, Ahultasuna

XXE erako ahultasuna IBMren Sterling B2B Integrator-en

Argitalpen data: 2019/03/27

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM Sterling B2B Integrator, 6.0.0.0 bertsioa

Azalpena:

XML External Entity Injection (XXE) erako kritikotasun altuko ahultasun bat aurkitu da Sterling B2B Integrator Standard Edition produktuan.

Konponbidea:

- IBM Sterling B2B Integrator-en 6.0.0.1 bertsioa deskargatzea.

Xehetasuna:

- IBM Sterling B2B Integrator Standard Edition-ek *XML External Entity Injection* (XXE) erako eraso bat jasan lezake XML datuak prozesatzean. Urruneko erasotzaile batek ahultasun hori balia lezake informazio sentikorra agerian uzteko edo memoriaren baliabideak kontsumitzeko. Ahultasun horretarako CVE-2019-4043 identifikatzailea erreserbatu da.

Etiketak: IBM, Ahultasuna

Hainbat ahultasun TIBCOren produktuetan

Argitalpen data: 2019/03/27

Garrantzia: Handia

Kaltetutako baliabideak:

- AWSrako TIBCO Data Science, 6.4.0 eta lehenagoko bertsioak.
- TIBCO Spotfire Data Science, 6.4.0 eta lehenagoko bertsioak.

Azalpena:

TIBCOk bere hainbat produkturi eragiten dieten 3 ahultasun argitaratu ditu. Horien bitartez erasotzaile batek web zerbitzariaren osagairako sarbidea lor lezake pribilegioekin, datuak aldatu edo ezabatu litzake, eta identitatearen ordezpena egin.

Konponbidea:

- AWSrako TIBCO Data Science, 6.4.1 edo goragoko bertsiora eguneratzea.
- TIBCO Spotfire Data Science, 6.4.1 edo goragoko bertsiora eguneratzea.

Xehetasuna:

Ahultasun horietako batzuk arrakastaz baliatuz gero, erabiltzaile batek ondokoak egin litzake:

- *Cross-site scripting* (XSS) bitartez pribilegiodun erabiltzaileentzat eskuragarri dauden web interfazeko gaitasun guztietara sarbidea lortzea. Ahultasun horretarako CVE-2019-8987 identifikatzailea erabili da.
- Kaltetutako sisteman bere pribilegioak eskalatzea, eta horrela babestutako datuak aldatu eta ezabatzea. Ahultasun horretarako CVE-2019-8988 identifikatzailea erabili da.

- Bere kontua faltsutzea eta identitatearen ordezpena egitea. Ahultasun horretarako CVE-2019-8989 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna.

Hainbat ahultasun Tableau Desktop-en

Argitalpen data: 2019/03/27

Garrantzia: Handia

Kaltetutako baliabideak:

- Tableau Desktop, Mac eta Windows sistema eragileetarako:
-
    - 10.1etik 10.1.22 bertsiora
    - 10.2tik 10.2.18 bertsiora
    - 10.3tik 10.3.18 bertsiora
    - 10.4tik 10.4.14 bertsiora
    - 10.5etik 10.5.13 bertsiora
    - 2018.1etik 2018.1.10 bertsiora
    - 2018.2tik 2018.2.7 bertsiora
    - 2018.3tik 2018.3.4 bertsiora
    - 2019.1etik 2019.1.0 bertsiora (Tableau Server-en 2019.1.1 bertsioa geldiarazi egin zen)
    - 2019.1etik 2019.1.1 bertsiora

Azalpena:

Tableau-k Tableau Desktop-i eragiten dioten hiru ahultasunen berri eman du. Horiek baliatuz kodea urrunetik exekuta liteke eta datuak erakutsi baimenik gabeko erabiltzaileei.

Konponbidea:

- Tableau Desktop-ek ahultasun horiek arintzen dituzten hainbat eguneraketa argitaratu ditu, bertsioaren eta sistema eragilearen arabera. Bertsioa ondorengo zerrendan ikus daiteke:
-
    - 10.1.23 bertsioa
    - 10.2.19 bertsioa
    - 10.3.19 bertsioa
    - 10.4.15 bertsioa
    - 10.5.14 bertsioa
    - 2018.1.11 bertsioa
    - 2018.2.8 bertsioa
    - 2018.3.5 bertsioa
    - 2019.1.2 bertsioa

Xehetasuna:

- Ahultasun batek informazioa *thumbnail*-etan (irudi txikiak) erakustea ahalbidetzen du. Lan liburu batean horiek ikus ditzakeen erabiltzaile batek horren irudi estatiko bat ikusi ahal izango du, argitaratu zen unean zen bezalakoa. Irudi horrek izan litzake erabiltzaile "ikusleak" ikusi beharko ez lituzkeen irudiak.
- Mac-en Tableau Desktop-en bidez asmo gaiztoko Web Datuen Konektore batera konektatzen den erabiltzaile batek memoriaren hondatze erako ahultasuna eragin lezake. Ahultasun hori baliatuko lukeen erasotzaile batek kode arbitrarioa exekuta lezake edo blokeo bat eragin.
- Webgune batean autentifikatzeko NTLM protokoloa erabiltzen denean, mugez kanpoko irakurketa eta idazketa gerta litezke. Horrek kodea urrunetik exekutatzea edo blokeo bat gertatzea eragin lezake. Tableau Server-en asmo gaiztoko liburu bat irekitzeak edo asmo gaiztoko instantzia batera konektatzeak ahultasun hori eragin dezakete. Ahultasun hori "libcurl" liburutegiarekin lotuta dago eta CVE-2018-16890 eta CVE-2019-3822 identifikatzaileak esleitu zaizkio.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna F5en BIG-IQ Centralized Management-en

Argitalpen data: 2019/03/28

Garrantzia: Handia

Kaltetutako baliabideak:

- BIG-IQ Centralized Management, 5.0.0tik 5.1.0ra bitarteko bertsioak.

Azalpena:

F5ek larritasun altuko ahultasun bat aurkitu du bere BIG-IQ Centralized Management produktuari eragiten diona.

Konponbidea:

- BIG-IQ Centralized Management 5.2.0 bertsiora eguneratzea, softwarearen deskarga zentrotik.

Xehetasuna:

- *XML External Entity* (XXE) erako ahultasun bat aurkitu da *libexpat* liburutegian 2.2.0 eta lehenagoko bertsioetan. Hori baliatuz erasotzaileek begizta infinitu bat eragin lezakete XML analizatzailean, DTD batetik (Document Type Definition) gaizki sortutako kanpoko entitateko adierazpen bat erabiliz. Ahultasun horretarako CVE-2017-9233 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna.

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/03/28

Garrantzia: Handia

Kaltetutako baliabideak:

- Cisco IOS edo IOS XE Software:
  - web server funtzioa gaituta duenean.
  - Cisco Plug-and-Play (PnP) gaituta eta abiatuta duenean.
  - NBAR eragiketetarako konfiguratuta dagoenean.
  - hauekin konfiguratuta dagoenean: NAT64 (Stateless edo Stateful), Address-en Mapping eta Port Using Translation (MAP-T), edo Address-en Mapping eta Port Using Encapsulation (MAP-E).
  - ISDN (RDSI) interfaze batekin konfiguratuta dagoenean.
  - IP SLA eragiketetarako konfiguratuta dagoenean.
  - Cisco ETA funtzioa erabiltzeko konfiguratuta dagoenean.
- Switches Cisco Catalyst 4500/4500X Series.
- Sierra Wireless WWAN cellular interfazea honako hauekin:
  - Cisco IOS Software Release 15.8(3)M.
  - Cisco IOS XE Software Release 16.10.1.
- Cisco ASR 900 RSP3, Cisco IOS XE softwarea exekutatu eta OSPFv2 routing eta OSPF Message Digest 5 (MD5) cryptographic authentication-erako konfiguratuta daudenean.

Azalpena:

Ciscok 23 ahultasun argitaratu ditu, horietatik 17 larritasun altukoak eta 6 larritasun ertainekoak.

Konponbidea:

- Ciscok ahultasunak konpontzen dituzten hainbat konponbide argitaratu ditu, kaltetutako produktuaren arabera. Eguneraketak eskuragarri daude Cisco softwarearen deskarga panelean.

Xehetasuna:

Larritasun altuko ahultasunak ondokoak dira, bakoitzari esleitutako identifikatzailea eta guzti:

- Informazioa zabaltzea: CVE-2019-1742.
- Komandoen injekzioa: CVE-2019-1745, CVE-2019-1756 eta CVE-2019-1755.
- Zerbitzua ukatzea: CVE-2019-1747, CVE-2019-1749, CVE-2019-1738, CVE-2019-1739, CVE-2019-1740, CVE-2019-1751, CVE-2019-1752, CVE-2019-1737, CVE-2019-1750, CVE-2019-1741 eta CVE-2019-1746.
- Ziurtagiriaren baliozkotze ez-nahikoa: CVE-2019-1748.
- Pribilegioen eskalatzea: CVE-2019-1754 eta CVE-2019-1753.
- Fitxategi arbitrarioen igoera: CVE-2019-1743.

Larritasun ertaineko ahultasunetarako honako identifikatzaileak erabili dira: CVE-2019-1760, CVE-2019-1758, CVE-2019-1757, CVE-2019-1762, CVE-2019-1761 eta CVE-2019-1759.

Etiketak: Eguneraketa, Cisco, Ahultasuna.

Hainbat ahultasun GnuTLS liburutegian

Argitalpen data: 2019/03/28

Garrantzia: Handia

Kaltetutako baliabideak:

- GnuTLS liburutegia, 3.5.8 eta lehenagoko bertsioetatik 3.6.7ra bitartekoak.

Azalpena:

Kritikotasun altuko bi ahultasun aurkitu dira, horietako bat Google Project Zero-ko Travis Ormandy ikertzaileak aurkitutakoa da. Erasotzaile batek zerbitzariaren ustekabeko itxiera eragin lezake edo ziurtagiriak arriskuan jarri.

Konponbidea:

- GnuTLS 3.6.7 edo geroagoko bertsioetara eguneratzea.

Xehetasuna:

- Gaizki sortutako TLS1.3 mezu asinkrono bat bidaltzen duen erasotzaile batek zerbitzariaren ustekabeko itxiera eragin lezake, erakuslerako sarbide ez-baliagarri baten bidez. Ahultasun horretarako CVE-2019-3836 identifikatzailea erreserbatu da.
- Ziurtagiriak egiaztatzeko APIak duen askapen bikoitz baten (*double free*) eraginez sortzen den memoriaren hondatzeak ziurtagiriak arriskuan jar litzake. X.509 ziurtagiriak egiaztatzen dituen edozein aplikazio, bezero nahiz zerbitzari izan, kaltetuta dago. Ahultasun horretarako CVE-2019-3829 identifikatzailea erabili da.

Etiketak: Eguneraketa, SSL/TLS, Ahultasuna.

Hainbat ahultasun VMwareren produktuetan

Argitalpen data: 2019/03/29

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- VMware vCloud Director for Service Providers (vCD), 9.5.x bertsioa;
- VMware vSphere ESXi (ESXi), 6.0, 6.5 eta 6.7 bertsioak edozein plataformatan;
- VMware Workstation Pro / Player (Workstation), 14.x eta 15.x bertsioak edozein plataformatan;
- VMware Fusion Pro / Fusion (Fusion), 10.x eta 11.X bertsioak OSXen.

Azalpena:

VMwarek bere produktu batzuei eragiten dieten 5 ahultasunen berri eman du.

Konponbidea:

- Zerbitzu hornitzaileentzako VMware vCloud Director (vCD), 9.5.0.3 bertsiora eguneratzea;
- VMware vSphere ESXi (ESXi):
-
    - 6.0 bertsioaren kasuan, ESXi600-201903001 partxea aplikatzea
    - 6.5 bertsioaren kasuan, ESXi650-201903001 partxea aplikatzea
    - 6.7 bertsioaren kasuan, ESXi670-201903001 partxea aplikatzea
- VMware Workstation Pro (Workstation):
    - 14.x bertsioen kasuan, 14.1.7ra eguneratzea
    - 15.x bertsioen kasuan, 15.0.4ra eguneratzea
- VMware Workstation Player (Workstation):
    - 14.x bertsioen kasuan, 14.1.7ra eguneratzea
    - 15.x bertsioen kasuan, 15.0.4ra eguneratzea
- VMware Fusion Pro / Fusion (Fusion):
    - 10.x bertsioen kasuan, 10.1.6 bertsiora eguneratzea
    - 11.x bertsioen kasuan, 11.0.3 bertsiora eguneratzea

Xehetasuna:

- Zerbitzu hornitzaileentzako VMware vCloud Director-ek urruneko saioaren bahiketa erako ahultasun bat dauka *Tenant* eta *Provider* atarietan. Ahultasun hori baliatuz asmo gaiztoko erasotzaile bat atari horietara sar liteke, une horretan saioa hasi duen erabiltzaile bat dela irudikatuz. Ahultasun horretarako CVE-2019-5523 identifikatzailea erreserbatu da.
- USB 1.1 kontrolatzaile birtual bat duen VMware ESXi, Workstation edo Fusion-en makina birtual batera sarbidea duen erasotzaile batek mugaz kanpoko irakurketa/idazketa erako edo *Time-of-check Time-of-use* (TOCTOU) erako ahultasun batzuk balia litzake. Horrela *host*-ean kodea exekuta lezake. Ahultasun horietarako CVE-2019-5518 eta CVE-2019-5519 identifikatzaileak erreserbatu dira.
- VMware Workstation eta Fusion-ek mugez kanpoko idazketa erako ahultasun bat daukate e1000 sare egokitzaile birtualean. Hori baliatuz erasotzaile batek kodea exekuta lezake *host*-ean. Ahultasun horretarako CVE-2019-5524 identifikatzailea erreserbatu da.
- VMware Workstation eta Fusion-ek mugez kanpoko idazketa erako ahultasun bat daukate e1000 eta e1000e sare egokitzaile birtualetan. Hori baliatuz erasotzaile batek kodea exekuta lezake host-ean, baina probableagoa da zerbitzuaren ukapen egoera (DoS) eragitea. Ahultasun horretarako CVE-2019-5515 identifikatzailea erreserbatu da.
- VMware Fusion-ek autentifikazioaren gabezia erako ahultasun bat dauka *web socket* baten bidez sar daitekeen APIetan. Erasotzaile batek ahultasun hori balia lezake *host*-aren erabiltzailea engainatuz JavaScript bat exekuta dezan, VMware Tools instalatuta dagoen ekipo gonbidatuan baimenik gabeko funtzioak egiteko xedeaz. Ahultasun horretarako CVE-2019-5514 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna