2019ko Ekainaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun HPE Smart Update Manager-en

Argitalpen data: 2019/06/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- HPE Smart Update Manager (SUM), 8.4 bertsioa baino lehenagokoak

Azalpena:

HPEk bere HPE Smart Update Manager (SUM) produktuak dituen bi ahultasunen berri eman du, bat baimenik gabeko pribilegio lokalen eskalatze erakoa, eta bestea baimendu gabeko urruneko sarbide erakoa.

Konponbidea:

- 8.4 edo goragoko bertsiora eguneratzea

Xehetasuna:

- HPE Smart Update Manager-ek (SUM) duen ahultasuna baliatuz baimendu gabeko sarbidea egitea lor liteke. Ahultasun horretarako CVE-2019-11988 identifikatzailea erreserbatu da.
- HPE Smart Update Manager-ek (SUM) duen ahultasuna baliatuz pribilegio lokalen baimenik gabeko eskalatzea egin liteke. Ahultasun horretarako CVE-2019-11987 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, HP, Ahultasuna

Hainbat ahultasun IBMren Intelligent Operations Center-en

Argitalpen data: 2019/06/03

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM® Intelligent Operations Center, 5.1.0tik 5.2.0ra bitarteko bertsioak
- Emergency Management-erako IBM® Intelligent Operations Center, 5.1.0tik 5.1.0.6ra bitarteko bertsioak
- Waternamics-erako IBM® Water Operations, 5.1.0tik 5.2.1.1erako bertsioak

Azalpena:

Intelligent Operations Center-i (IOC) eragiten dioten zerbitzuaren ukapen erako eta fitxategien baliozkotzeko oker erako bi ahultasunen berri eman da.

Konponbidea:

- IBM® Intelligent Operations Center, 5.2.0 bertsioa, PO08061 interim fix aplikatzea
- IBM® Intelligent Operations Center, 5.1.0tik 5.1.0.14ra bitarteko bertsioak, interim fix PO08131 aplikatzea
- IBM® Intelligent Operations Center, 5.1.0tik 5.1.0.14ra bitarteko bertsioak, interim fix PO08061 aplikatzea

Xehetasuna:

- IBM Intelligent Operations Center-ek (IOC) duen ahultasun bat baliatuz, autentifikatutako erabiltzaile batek erabiltzaile arbitrarioak sor litzake, IDen kudeaketan arazoak eragin litzaketenak, eta horiek, azkenean, kodea exekutatu lezakete. Ahultasun horretarako CVE-2019-4066 identifikatzailea erreserbatu da.

- IBM Intelligent Operations Center-ek (IOC) fitxategi moten baliozkotze okerra eragiten duen ahultasun bat dauka. Hori baliatuz erasotzaile batek asmo gaiztoko edukia karga lezake. Ahultasun horretarako CVE-2019-4069 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Dell EMC OpenManage System Administrator-en (OMSA)

Argitalpen data: 2019/06/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Dell EMC OpenManage System Administrator (OMSA):
  - 9.1.0.3 baino lehenagoko bertsioak
  - 9.2.0.4 baino lehenagoko bertsioak

Azalpena:

Dell-ek bi ahultasunen berri eman du: bat larritasun kritikokoa, web parametroen manipulazio erakoa; eta beste bat larritasun altukoa, XXE (XML External Entity) injekzio erakoa.

Konponbidea:

Dell-ek produktua eguneratzea gomendatzen du bere deskargen zentrotik ondoko bertsioetako batera:

- 9.1.0.3 edo berriagoa
- 9.2.0.4 edo berriagoa
- 9.3.0 edo berriagoa

Xehetasuna:

- XXE (XML External Entity) injekzio erako ahultasun bat baliatuz, autentifikatu gabeko erasotzaile batek zerbitzariko fitxategi arbitrarioak irakur litzake dokumentu motako (DTD) definizioak ematerakoan, bereziki diseinatutakoak XML eskaera batean. Ahultasun horretarako CVE-2019-3722 identifikatzailea erreserbatu da.
- Web parametroen manipulazio erako ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek OMSArako web eskarien parametroak manipula litzake, eta fitxategi arbitrarioak sortu edukia hutsik daukatela, edo edozein fitxategitako edukia ezaba lezake. Horren arrazoia da sarrera parametroen baliozkotze desegokia. Ahultasun horretarako CVE-2019-3723 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Autentifikazioa saihestea IBM PureApplication System-en

Argitalpen data: 2019/06/04

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM PureApplication System, ondoko bertsioak:
  - 2.2.3.0
  - 2.2.3.1
  - 2.2.3.2
  - 2.2.4.0
  - 2.2.5.0
  - 2.2.5.1
  - 2.2.5.2
  - 2.2.5.3

Azalpena:

IBMk bere PureApplication System produktuari eragiten dion ahultasun baten berri eman du. Hori baliatuz administratzaile sarbidea lor liteke.

Konponbidea:

- IBM PureApplication System V2.2.6.0 bertsiora eguneratzea.

Xehetasuna:

- IBM Pure Application System-ek sarbide lokala lukeen autentifikatutako erabiltzaile bati ahalbidetuko lioke autentifikazioa saihestea eta administratzaile sarbidea eskuratzea. Ahultasun horretarako CVE-2019-4241 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Ahultasuna IBMren Jazz for Service Management-

en (JazzSM)

Argitalpen data: 2019/06/05

Garrantzia: Handia

Kaltetutako baliabideak:

- Jazz for Service Management (JazzSM), 1.1.3 - 1.1.3.2 bertsioak

Azalpena:

IBMk bere Jazz for Service Management (JazzSM) produktuari eragiten dion ahultasun baten berri eman du. Hori baliatuz, urruneko erasotzaile batek phishing erasoak egin litzake birbideratze irekiko eraso bat erabiliz.

Konponbidea:

- Install 1.1.3-TIV-JazzSM-multi-FP003 partxea aplikatzea

Xehetasuna:

- IBM Jazz for Service Management-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 erakutsitako URLa faltsutu lezake, eta erabiltzaile bat fidagarria zaion asmo gaiztoko webgune batera birbideratu. Horri esker erasotzaileak informazio sentikorra eskura lezake edo biktimaren aurkako eraso berriak egin. Ahultasun horretarako CVE-2019-4201 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

SQLi eta CSRF erako ahultasunak phpMyAdmin-en

Argitalpen data: 2019/06/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- 4.8.6 (CVE-2019-11768) baino lehenagoko phpMyAdmin-en bertsioak
- 4.9.0 baino lehenagoko phpMyAdmin bertsio guztiak, gutxienez 4.0 (CVE-2019-12616) bertsioaz geroztikakoak

Azalpena:

Bi ahultasun aurkitu dira phpMyAdmin-en, horietako bat kritikoa:

- phpMyAdmin-eko lantaldeko kidea den William Desportes-ek Designer funtzioak duen SQL injekzio erako ahultasun baten berri eman du.
- Mauro Tempestak kritikotzat kalifikatutako ahultasun bat aurkitu zuen, CSRF erakoa (Cross-Site Request Forgery edo gune gurutzatuetan eskaeraren faltsutzea), saio hasierako formularioan.

Konponbidea:

Produktua eguneratzea edo partxeak aplikatzea gomendatzen da:

- phpMyAdmin 4.8.6 bertsiora edo berriago batera eguneratzea edo partxea aplikatzea SQL injekzio erako ahultasuna konpontzeko.
- phpMyAdmin 4.9.0 bertsiora edo berriago batera eguneratzea edo partxea aplikatzea CSRF erako ahultasuna konpontzeko.

Xehetasuna:

- SQL injekzio erako ahultasunaren ondorioz, bereziki diseinatutako datu base baten izena erabil daiteke era horretako eraso bat abiatzeko. Ahultasun horretarako CVE-2019-11768 kodea erabili da.
- CSRF erako ahultasuna baliatuz, erasotzaile batek erabiltzailea engaina lezake, adibidez biktimaren phpMyAdmin datu basera apuntatzen duen formularioan hautsita dagoen < img > etiketa baten bidez. Horrela erasotzaileak karga baliagarri edo payload bat eman lezake (INSERT edo DELETE jarraibide zehatz baten modura). Ahultasun horretarako CVE-2019-12616 kodea erabili da.

Etiketak: Eguneraketa, Ahultasuna

DoS eta kodearen urruneko exekuzioa Cisco-ren hainbat produktutan

Argitalpen data: 2019/06/06

Garrantzia: Handia

Kaltetutako baliabideak:

- Expressway Series, sarbide mugikorrerako eta urruneko sarbiderako konfiguratuta IM&P Service-rekin, X8.1etik X12.5.2ra bitarteko bertsioak
- TelePresence VCS, sarbide mugikorrerako eta urruneko sarbiderako konfiguratuta IM&P Service-rekin, X8.1etik X12.5.2ra bitarteko bertsioak
- Unified Communications Manager IM&P Service, honako bertsioak:
  - 10.5(2)
  - 11.5(1)
  - 12.0(1)
- Cisco Industrial Network Director, 1.6.0 baino lehenagoko bertsioak

Azalpena:

Ciscok bere produktu batzuei eragiten dieten zerbitzuaren ukapen erako ahultasun bat eta kodearen exekuzio arbitrarioko beste bat argitaratu ditu.

Konponbidea:

Ciscok hainbat eguneraketa argitaratu ditu, kaltetutako produktuaren arabera, bere deskargen zentroan eskuragarri.

- Expressway Series, sarbide mugikorrerako eta urruneko sarbiderako konfiguratuta IM&P Service-rekin, X12.5.3 edo goragoko bertsio batera eguneratu.
- TelePresence VCS, sarbide mugikorrerako eta urruneko sarbiderako konfiguratuta IM&P Service-rekin, X12.5.3 edo goragoko bertsio batera eguneratu.
- Unified Communications Manager IM&P Service:
  - 10.5(2) bertsioaren kasuan, 11.5(1) SU6 edo 12.5(1) bertsioetara eguneratu
  - 11.5(1) bertsioaren kasuan, 11.5(1) SU6 bertsiora eguneratu
  - 12.0(1) bertsioaren kasuan, 12.5(1) bertsiora eguneratu
- Cisco Industrial Network Director, 1.6.0 edo goragoko bertsiora eguneratu.

Detalle:

- Urruneko erasotzaile batek gaizki sortutako autentifikazio eskaera bat bidal lezake *Extensible Messaging and Presence Protocol*-era (XMPP), eta horrela autentifikazio zerbitzuaren ustekabeko berrabiatzea eragin eta zerbitzuaren ukapen egoera (DoS) sortu. Ahultasun horretarako CVE-2019-1845 identifikatzailea erabili da.
- Aplikazioan kargatutako fitxategien baliozkotze oker bat baliatuz, administratzaile pribilegioak lituzkeen autentifikatutako erasotzaile batek fitxategi arbitrario bat karga lezake eta kodea exekutatu. Ahultasun horretarako CVE-2019-1861 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun VMware produktuetan

Argitalpen data: 2019/06/06

Garrantzia: Handia

Kaltetutako baliabideak:

- VMware Tools eguneratu 10.3.10 bertsiora
- Linuxeko VMware Workstation Pro / Player, 15.x bertsioa

Azalpena:

VMware-k VMware Tools-ek duen mugez kanpoko irakurketa erako ahultasun baten berri eta Workstation-ek duen askapenaren ondoreneko memoriaren erabilera erako beste ahultasun baten berri eman du.

Konponbidea:

- VMware Tools eguneratu 10.3.10 bertsiora
- Workstation Pro / Player eguneratu 15.1.0 bertsiora

Xehetasuna:

- Windowsen ekipo gonbidatuetan vmtools-ekin batera instalatzen den vm3dmp kontrolatzaileak duen mugez kanpoko irakurketa erako ahultasun bat baliatuz, administratzaile sarbiderik ez duen erasotzaile lokal batek kerneleko informazioa iragaz lezake edo zerbitzuaren ukapen eragin Windowsen ekipo gonbidatu berean. Ahultasun horretarako CVE-2019-5522 identifikatzailea erreserbatu da.
- VMware Workstation-en askapenaren ondoreneko memoriaren erabilpen erako ahultasuna baliatuz, makina gonbidatuan erabiltzaile pribilegioak lituzkeen erasotzaile batek kodea exekuta lezake lan estazioa instalatuta dagoen Linux host-ean. Ahultasun horretarako CVE-2019-5525 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

SAPen 2019ko ekaineko segurtasun eguneraketa

Argitalpen data: 2019/06/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa
- Solution Manager, 7.2 bertsioa
- SAP E-Commerce (Business-to-Consumer application), honako bertsioak: SAP-CRMJAV, SAP-CRMWEB, SAP-SHRWEB, SAP-SHRJAV, SAP-CRMAPP, SAP-SHRAPP 7.30, 7.31, 7.32, 7.33, 7.54
- SAP R/3 Enterprise Application, honako bertsioak: EA-APPL 600, 602, 603, 604, 605, 606, 616, 617
- SAP BusinessObjects Business Intelligence Platform (Administration Console), 4.2, 4.3 bertsioak
- SAP NetWeaver Process Integration (PI Integration Builder Web UI), honako bertsioak: SAP_XIESR: 7.10etik 7.11ra bitartekoak, 7.20, 7.30, 7.31, 7.40, 7.50; SAP_XITOOL: 7.10etik 7.11ra bitartekoak, 7.30, 7.31, 7.40, 7.50, SAP_XIPCK 7.10etik 7.11ra bitartekoak, 7.20, 7.3
- SAP Work Manager and SAP Inventory Manager, SAP Work Manager-en 6.3.0, 6.4.0, 6.5 bertsioak
- SAP NetWeaver AS ABAP Platform, 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 7.21, 7.45, 7.49, 7.53, 7.73
- SAP NetWeaver Process Integration, versiones SAP_XIESR-en honako bertsioak: 7.10etik 7.11ra bitartekoak, 7.20, 7.30, 7.31, 7.40, 7.50; SAP_XITOOL: 7.10etik 7.11ra bitartekoak, 7.20, 7.30, 7.31, 7.40, 7.50
- SAP HANA Extended Application Services (advanced model), 1 bertsioa

- SAP Enterprise Financial Services, honako bertsioak: SAPSCORE 1.13, 1.14, 1.15; S4CORE 1.01, 1.02, 1.03; 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; Bank/CFM 4.63_20

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.
- Larritasun altuko ahultasuna konpontzeko fabrikatzailearen oharra kontuan hartzea gomendatzen da. Bertan hainbat urrats zehazten dira: batetik, nola instalatu behar den ahultasuna konpontzen duen softwarea, bestetik, aldez aurretik aplikatu behar diren SAPen beste segurtasun oharrekiko mendekotasunak, eta azkenik, kredentzialak modu egokian babesteko eta zifratzeko nola egin behar den urratsez urrats.

Xehetasuna:

SAPek segurtasun partxeei buruz argitaratzen duen hileroko komunikatuan 11 segurtasun ohar eta 3 eguneraketa eman ditu ezagutzera. Horietatik 1 larritasun kritikokoa da, 1 larritasun altukoa, 11 larritasun ertainekoak eta 1 larritasun baxukoa.

Argitaratutako ahultasun motak honako hauek dira:

- Baimenaren egiaztapen gabeziako 5 ahultasun.
- Informazio zabalkundeko 5 ahultasun..
- Pribilegioen eskalatze erako ahultasun bat.
- Beste era batzuetako 2 ahultasun

Kritikotzat eta altutzat kalifikatutako segurtasun oharrak honi buruzkoak dira:

- SAP Business Client exekutatzen ari denean zaharkituta dagoen Chromium batean, erasotzaile batek bere erabiltzaile baterako sarbidea lor lezake asmo gaiztoko Javascript kodea exekutatzeko. Ustiatua izaten ari den Chromium ahultasunaren baitan dago benetako eragina.

- Ahultasun bat baliatuz, erasotzaile batek baliagarriak diren erabiltzaile kredentzialak eskura litzake, eta erabiltzaile kontu pribilegiatuak sortzeko gaitasuna eskuratu. Horrek eragin handia dauka konfidentzialtasunean. Larritasun altuko ahultasun horretarako CVE-2019-0291 identifikatzailea erabili da.

Gainerako ahultasunetarako erabilitako identifikatzaileak honako hauek dira: CVE-2019-0308, CVE-2019-0311, CVE-2019-0303, CVE-2019-0315, CVE-2019-0314, CVE-2019-0304, CVE-2018-0312, CVE-2019-0316, CVE-2019-0305, CVE-2019-0306, CVE-2019-2484 eta CVE-2019-0307.

Etiketak: Eguneraketa, SAP, Ahultasuna

Microsoften 2019ko ekaineko segurtasun buletina

Argitalpen data: 2019/06/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Adobe Flash Player
- Microsoft Windows
- Internet Explorer
- Microsoft Edge
- Microsoft Office eta Microsoft Office Services eta Web Apps
- ChakraCore
- Skype para Business y Microsoft Lync
- Microsoft Exchange Server
- Azure

Azalpena:

Segurtasun eguneraketei buruzko Microsoften hileroko argitalpenean 87 ahultasun jaso dira, 21 kritiko gisa sailkatu dira eta 66 garrantzitsu gisa.

Konponbidea:

- Dagozkien segurtasun eguneraketak instalatzea. Eguneraketei beraiei buruzko instalazioaren informazio orrian hori egiteko metodo ezberdinei buruzko argibideak daude.

Xehetasuna:

Argitaratutako ahultasun motak honako hauek dira:

- Kodearen urruneko exekuzioa.
- Informazioa zabaltzea.
- Pribilegioen igoera.
- Zerbitzuaren ukapena.
- Segurtasunari ihes egitea.
- Ordezpena.
- Faltsutzea.

Etiketak: Eguneraketa, Microsoft, Nabigatzailea, Windows

Hainbat ahultasun Intel produktuetan

Argitalpen data: 2019/06/12

Garrantzia: Handia

Kaltetutako baliabideak:

- Intel® Accelerated Storage Manager in Intel® RSTe, 5.5.0.2015 baino lehenagoko bertsioak.
- Windowserako Intel® RAID Web Console 3, 4.186 eta lehenagoko bertsioak
- Intel® NUC Kit, ikusi erreferentzien atala kaltetutako bertsioak zein diren jakiteko
- Intel® Compute Card, ikusi erreferentzien atala kaltetutako bertsioak zein diren jakiteko
- Intel® Compute Stick, ikusi erreferentzien atala kaltetutako bertsioak zein diren jakiteko
- Open CIT y OpenAttestation, bertsio guztiak
- Intel® Omni-Path Fabric Manager GUI, 10.9.2.1.1 baino lehenagoko bertsioak
- Intel® PROSet/Wireless WiFi Software, Microsoft Windows 7, 8.1 eta 10erako 21.10 baino lehenagoko bertsioak
- Intel® Turbo Boost Max Technology 3.0 driver, 1.0.0.1035 eta lehenagoko bertsioak
- Intel® SGX Linux client driver, 2.5 baino lehenagoko bertsioak
- Intel® SGX DCAP Linux driver, 1.1 baino lehenagoko bertsioak
- Windows 10erako ITE Tech* Consumer Infrared Driver, 5.4.3.0 baino lehenagoko bertsioak
- Intel® Chipset Device Software (INF Update Utility), 10.1.1.45 baino lehenagoko bertsioak

Azalpena:

Intelek bere produktu batzuei eragiten dieten hainbat ahultasunen berri eman du.

Konponbidea:

- Produktuaren azken bertsiora eguneratzea hemen: Intelen softwarearen deskarga zentroa.

Xehetasuna:

Kritikotasun altuko ahultasunak ondokoak dira:

- Intel® RSTe-rako Intel® Accelerated Storage Manager-en web interfazeak duen Reflected XSS erako ahultasun bat baliatuz, autentifikaziorik gabeko erabiltzaile batek zerbitzuaren ukapen egoera eragin lezake sare bidezko sarbide baten bitartez. Ahultasun horretarako CVE-2019-0130 identifikatzailea erreserbatu da.
- Intel® NUCen firmware-ak hainbat ahultasun ditu. Horiek baliatuz erasotzaile batek pribilegioen eskalatzea egin lezake, zerbitzuaren ukapen egoera sortu eta informazioa hedatu. Gainerako ahultasunetarako ondoko identifikatzaileak erreserbatu dira: CVE-2019-11123, CVE-2019-11124, CVE-2019-11125, CVE-2019-11126, CVE-2019-11127, CVE-2019-11128 eta CVE-2019-11129.
- Intel® RWC3rako zerbitzu APIak duen saioaren baliozkotze ez-nahikoaren ahultasun bat baliatuz, autentifikatutako erasotzaile batek pribilegioen eskalatzea egin lezake sare bidezko sarbide baten bitartez. Ahultasun horretarako CVE-2019-11119 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako ondoko identifikatzaileak erreserbatu dira: CVE-2019-0175, CVE-2019-0177, CVE-2019-0178, CVE-2019-0179, CVE-2019-0180, CVE-2019-0181, CVE-2019-0182, CVE-2019-0183, CVE-2019-11092, CVE-2019-11117, CVE-2019-0136, CVE-2019-0164, CVE-2019-0157, CVE-2018-3702, CVE-2019-0128 eta CVE-2019-0174.

Etiketak: Eguneraketa, Ahultasuna

Joomla!-ren segurtasun eguneraketa

Argitalpen data: 2019/06/12

Garrantzia: Txikia

Kaltetutako baliabideak:

Joomla! CMS, 3.6.0tik 3.9.6ra bitarteko bertsioak.

Azalpena:

Joomla!-k bi bertsio berri argitaratu ditu, 3.9.8 eta 3.9.7. Azken horretan bere nukleoak dituen kritikotasun txikiko hiru ahultasun konpontzen dira.

Konponbidea:

Bere webean eskuragarri dagoen azken bertsiora eguneratzea, 3.9.8. hain zuzen.

Xehetasuna:

3.9.7 bertsioan konpondutako ahultasunak honakoak dira:

- CSV datuen injekzio erako ahultasuna "com_actionslogs" osagaia esportatzean.
- XSS erako ahultasuna "subform" eremuan, sarreraren baliozkotze nahikorik ez dagoelako.
- Sarbide kontrolen eta ACLren erabilera okerragatik sortutako ahultasuna. Hori baliatuz, administratzaile ez diren erabiltzaileek "com_joomlaupdate" osagaia manipula dezakete.

Etiketak: Eguneraketa, CMS, Ahultasuna

Cross-Site Request Forgery erako ahultasuna Cisco IOS XE Software Weben

Argitalpen data: 2019/06/13

Garrantzia: Handia

Kaltetutako baliabideak:

HTTP Server ezaugarria gaituta daukaten Cisco IOS XE Software produktuak.

Azalpena:

Ciscok erabiltzailearen web interfazeari eragiten dion ahultasun baten berri eman du. Hori baliatuz autentifikatu gabeko urruneko erasotzaile batek Cross-Site Request Forgery (CSRF) eraso bat egin lezake.

Konponbidea:

Ciscok ez du inolako konponbiderik argitaratu ahultasun honetarako. Arintze neurri modura HTTP Server ezaugarria desgaitzea aholkatzen du "*no ip http server*" edo "*no ip http secure-server*" komandoen bidez.

Xehetasuna:

CSRF erako erasoen aurreko babes ez-nahiko bat balia lezake erasotzaile batek baldin eta interfazearen erabiltzaile bat konbentzitzen badu asmo gaiztoko esteka batera sar dadin. Horri esker, kaltetutako erabiltzaileak duen pribilegio maila berdinarekin ekintza arbitrarioak egin litzake, konfigurazioa aldatu, komandoak exekutatu edo gailua berrabiarazi. Ahultasun horretarako CVE-2019-1904 identifikatzailea erreserbatu da.

Etiketak: 0day, Cisco, Ahultasuna

Hainbat ahultasun IBMren produktuetan

Argitalpen data: 2019/06/17

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM InfoSphere Information:
  - Server, 11.3, 11.5 eta 11.7 bertsioak;
  - Governance Catalog, 11.3, 11.5 eta 11.7 bertsioak;
  - Server in Cloud, 11.5 eta 11.7 bertsioak;
  - Server Business Glossary, 9.1 bertsioa;
  - Server Metadata Workbench, 9.1 bertsioa.
- IBM Tivoli Netcool Impact, 7.1.0.0tik 7.1.0.15era bitarteko bertsioak.

Azalpena:

IBMk XXE (XML External Entity) injekzio eta kodearen urruneko exekuzio erako bi ahultasunen berri eman du, hurrenez hurren bere IBM InfoSphere Information Server eta IBM Tivoli Netcool Impact produktuei eragiten dietenak.

Konponbidea:

- InfoSphere Information Server:
  - 11.7 bertsioen kasuan, 11.7.1.0 eta 11.7.1.0 Enterprise Edition bertsioetara eguneratzea;
  - 11.5 bertsioaren kasuan, 11.5.0.2 eta 11.5 Service Pack 5 bertsioetara eguneratzea eta XMETA eta istool segurtasun partxeak aplikatzea;
  - 11.3 bertsioaren kasuan, 11.3.1.2 bertsiora eguneratzea eta XMETA eta istool segurtasun partxeak aplikatzea;
- InfoSphere Information Governance Catalog:
  - 11.5 bertsioaren kasuan, segurtasun partxea aplikatzea;
  - 11.3 bertsioaren kasuan, segurtasun partxea aplikatzea.
- Business Glossary eta Metadata Workbench: bertsio berri batera eguneratzea.
- IBM Tivoli Netcool Impact 7.1.0: fix pack 16 aplikatzea.

Xehetasuna:

- IBM InfoSphere Information Server ahula da XXE (XML External Entity) injekzio erako eraso baten aurrean XML datuak prozesatzen direnean. Urruneko erasotzaile batek ahultasun hori balia lezake informazio sentikorra agerian uzteko edo memoriaren baliabideak kontsumitzeko. Ahultasun horretarako CVE-2018-1845 identifikatzailea erreserbatu da.
- IBM Tivoli Netcool-ek ahalbidetzen du pribilegioen maila baxua duten erabiltzaileek komandoak urrunetik exekutatzea. Ahultasun horren eraginez sisteman kode arbitrarioa exekuta liteke, eta horrela bere kontrola hartu. Ahultasun horretarako CVE-2019-4103 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Netgear routerretan

Argitalpen data: 2019/06/17

Garrantzia: Handia

Kaltetutako baliabideak:

Wireless AC Router Nighthawk, honako modeloak:

- R7900, 1.0.3.14_10.0.40_BETA baino lehenagoko *firmware* bertsioa exekutatzen.
- R8000, 1.0.4.38_10.1.59_BETA baino lehenagoko *firmware* bertsioa exekutatzen.

Azalpena:

Cisco Talos-ek kritikotasun altuko bi ahultasun aurkitu ditu NETGEARen KCodes NetUSBrako *firmwarean*.

Konponbidea:

NETGEARek ahultasunak konpontzen dituzten bi eguneraketa argitaratu ditu:

- R7900, 1.0.3.14 - Hot Fix firmware bertsioa;

- R8000, 1.0.4.38 - Hot Fix firmware bertsioa.

Xehetasuna:

Aurkitutako ahultasunak baliatuz, urruneko erasotzaile batek *kernelaren* autentifikatu gabeko informazioa ezagutaraz lezake, eta memoriaren irakurketa arbitrarioa egin. Ahultasun horietarako CVE-2019-5016 eta CVE-2019-5017 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Ahultasuna

Sarbidearen kontrol desegoki erako ahultasuna Citrix-en AppDNAn

Argitalpen data: 2019/06/18

Garrantzia: Handia

Kaltetutako baliabideak:

AppDNA, 7.18 bertsioa eta lehenagokoak.

Azalpena:

Sarbidearen kontrol desegoki erako ahultasun bat aurkitu du Citrix-ek bere AppDNA produktuan.

Konponbidea:

Citrix-ek bezeroei aholkatzen die AppDNA 7 1906.1.0.0.472 eta goragoko bertsioetara eguneratzea eta IIS (Internet Information Services) konfiguratzea produktuaren dokumentazioan adierazten den moduan.

Xehetasuna:

AppDNAk duen ahultasun bat identifikatu da. Horren eraginez, sarbide kontrolak ez dira aplikatzen web kontsolara sartzean, eta horrek pribilegioak eskalatzea eta kodearen urruneko exekuzioa ahalbidetu litzake. Ahultasun horretarako CVE-2019-12292 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

TCPn oinarritutako zerbitzuaren ukapen erako ahultasunak Linux eta FreeBSDren Kernel-etan

Argitalpen data: 2019/06/18

Garrantzia: Handia

Kaltetutako baliabideak:

- Linuxen Kernelaren bertsioak:
  - SACK Panic: 2.6.29 bertsioaren berdinak edo berriagoak direnei eragiten die;
  - SACK Slowness: 4.15 bertsioa baino lehenagokoak;
  - Baliabideen gehiegizko kontsumoa: bertsio guztiak.
- RACK TCP (SACK Slowness) pila erabiltzen duten FreeBSD 12ren bertsioak.

Azalpena:

Netflixeko ikertzaileek lau ahultasun aurkitu dituzte, bat kritikotasun altukoa eta hiru kritikotasun ertainekoak. Ahultasun horien arrazoia TCP paketeetan segmentuaren tamaina maximoaren edo minimoaren (MSS) gaitasunak dira, bai eta TCPren (TCP SACK) ezagutza selektiboa ere. Urruneko erasotzaile batek ahultasun hori balia lezake zerbitzuaren ukapen egoera eragiteko.

Konponbidea:

- Linux sistema eragileen banaketa nagusietarako ahultasun horiek konpontzek dituzten eguneraketak argitaratu dira:
  - Debian: DSA-4465-1 segurtasun eguneraketaren paketeak instalatu;
  - Ubuntu: USN-4017-1 eta USN-4017-2 segurtasun eguneraketen paketeak instalatu;
  - RedHat: argitaratutako oharretan eskuragarri dauden eguneraketa paketeak instalatu;
  - SUSE sistema eragilearen kasuan oraindik ez da partxerik argitaratu, baina jakinarazi denaren arabera dagozkien partxeak eskainiko zaizkie zerbitzua duten banaketei;
- AWSren kasuan, egunerakeeta hauen berri eman da.
- FreeBSD 12 sistema eragileen kasuan ez dago partxe ofizialik, eta ondorioz Netflixeko ikertzaileek behin-behineko konponbide hauek proposatzen dituzte:
  - split_limit.patch partxea ezartzea eta net.inet.tcp.rack.split_limit-en sysctl-a zentzuzko balio batean finkatzea, SACK taularen tamaina mugatzeko;
  - Aldi baterako TCP RACK pila desgaitzea.

Xehetasuna:

Kritikotasun altuko ahultasunaren arrazoia da osokoen gainezkatzea eragin lezakeen aldatutako SACKen segida bat da, kernel panic bat sor lezakeena. Ahultasun horretarako CVE-2019-11477 identifikatzailea erreserbatu da.

Kritikotasun ertaineko gainerako ahultasunetarako CVE-2019-11478, CVE-2019-5599 eta CVE-2019-11479 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Komunikazioak, Linux, Ahultasuna

Kodearen urruneko exekuzio erako ahultasuna Oracle WebLogic Server-en

Argitalpen data: 2019/06/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Oracle WebLogic Server, 10.3.6.0.0, 12.1.3.0.0 eta 12.2.1.3.0 bertsioak.

Azalpena:

Oracle-k larritasun kritikoko ahultasun baten berri eman du, bere Oracle WebLogic Server produktuan kodearen urruneko exekuzioa ahalbidetzen duena.

Konponbidea:

Oracle-k erabiltzaile erregistratuei esteka bat eskaini die eskuragarri dauden partxeei eta horiek instalatzeko argibideei buruzko informazioa jasotzen duen dokumentazioa lortzeko.

Xehetasuna:

Oracle WebLogic Server-ek XMLDecoder-en bidez duen deserializazio erako ahultasun bat baliatuz, erasotzaile batek urrunetik eta autentifikaziorik gabe kodea exekuta lezake. Ahultasun horretarako CVE-2019-2729 identifikatzailea erabili da.

Etiketak: Eguneraketa, Oracle, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/06/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco SD-WAN Solution-en 18.3.6, 18.4.1 eta 19.1.0 bertsioak baino lehenagokoren bat exekutatzen duten Ciscoren ondorengo produktuak: :
  - vBond Orchestrator Software,
  - vEdge 100 Series Routers,
  - vEdge 1000 Series Routers,
  - vEdge 2000 Series Routers,
  - vEdge 5000 Series Routers,
  - vEdge Cloud Router Platform,
  - vManage Network Management Software,
  - vSmart Controller Software.
- Cisco DNA Center Software, 1.3 bertsioa baino lehenagokoak.
- Cisco TelePresence TC edo Cisco TelePresence CE software-ren bertsio ahul bat exekutatzen duten Ciscoren ondorengo produktuak:
  - Cisco TelePresence Integrator C Series,
  - Cisco TelePresence EX Series,
  - Cisco TelePresence MX Series,
  - Cisco TelePresence SX Series,
  - Cisco Webex Room Series.
- Cisco StarOS operating system-en bertsio ahul bat exekutatzen duten Ciscoren honako produktu hauek:
  - Cisco Virtualized Packet Core-Single Instance (VPC-SI),
  - Cisco Virtualized Packet Core-Distributed Instance (VPC-DI).
- Cisco vManage Network Management Software, Cisco SD-WAN Solution-en 18.4.0 bertsioa baino lehenagokoren bat exekutatzen.
- RV110W Wireless-N VPN Firewall, 1.2.2.4 baino lehenagoko bertsioak.
- RV130W Wireless-N Multifunction VPN Router, 1.0.3.51 baino lehenagoko bertsioak.
- RV215W Wireless-N VPN Router, 1.3.1.4 baino lehenagoko bertsioak.
- Cisco Prime Service Catalog Software, 12.1 Cumulative patch 10 bertsioa baino lehenagokoak.
- Cisco Meeting Server deployments, 2.2.14 eta 2.3.8 baino lehenagoko bertsioak exekutatzen.

Ciscok hainbat ahultasunen berri eman du. Horiek baliatuz kaltetutako produktuetan erasotzaile batek hainbat ekintza egin litzake: pribilegioak eskalatu, autentifikazioa saihestu, urruneko kodea exekutatu, zerbitzua ukatu edo cross-site request forgery (CSRF) erasoak egin.

Konponbidea:

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

Xehetasuna:

Larritasun kritikoko ahultasunak honakoak dira:

- Cisco SD-WAN Solution-en CLIen baimentzean betetze ez-nahiko bat baliatuz, erasotzaile bat gailuan autentifikatu liteke eta komandoak exekutatu pribilegioen eskalatzea egin ahal izateko. Horrela sistemaren konfigurazioan aldaketak egin litzake root erabiltzaile modura. Ahultasun horretarako CVE-2019-1625 identifikatzailea erabili da.
- Cisco Digital Network Architecture (DNA) Center-en sistemaren funtzionamendurako beharrezkoak diren ataketarako sarbide murrizketa ez-nahiko bat baliatuz, erasotzaile batek klusterraren zerbitzuetarako esleitutako azpi-sarera baimendu gabeko sare gailu bat konekta lezake, eta horrela kanpoko sarbideen aurrean babestu gabe dauden barne zerbitzuetara sarbidea lor lezake. Ahultasun horretarako CVE-2019-1848 identifikatzailea erabili da..

Larritasun altuko gainerako ahultasunetarako honako identifikatzaile hauek esleitu dira: CVE-2019-1878, CVE-2019-1869, CVE-2019-1626, CVE-2019-1624, CVE-2019-1843, CVE-2019-1874, CVE-2019-1623.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Zerbitzuaren ukapen erako ahultasuna Apache Tomcat-en

Argitalpen data: 2019/06/21

Garrantzia: Handia

Kaltetutako baliabideak:

- Apache Tomcat®, honako bertsioak:
  - 8.5.0tik 8.5.40ra bitartekoak;
  - 9.0.0.M1etik 9.0.19ra bitartekoak.

Azalpena:

Apachek osatugabe zegoen aurreko eguneraketa baterako zuzenketa bat argitaratu du, CVE-2019-0199 identifikatzailea zuen ahultasunarena, hain zuzen. Hori baliatuz erasotzaile batek hariak agortzea eta zerbitzua ukatzea (DoS) eragin lezake.

Konponbidea:

- 8.5.41 edo goragoko bertsiora eguneratzea.
- 9.0.20 edo goragoko bertsiora eguneratzea.

Xehetasuna:

- Eguneraketa honen bitartez idazketan zehar HTTP/2 konexio leihoaren agorpenerako osatugabe zegoen konponbide bat zuzentzen da. Konexio leihorako (stream 0) WINDOWS UPDATE mezurik ez bidaltzean, bezeroek eragin zezaketen zerbitzariaren aldeko hariak blokeatzea, zerbitzuaren ukapen egoera sortuz. Ahultasun horretarako CVE-2019-10072 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Apache, Ahultasuna

Hainbat ahultasun Liferay produktuetan

Argitalpen data: 2019/06/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Liferay Portal 7.1 CE GA3 eta zerbitzurik gabeko aurreko bertsioak.

Azalpena:

Liferay-k hainbat ahultasunen berri eman du, bat larritasun kritikokoa eta bost larritasun altukoak. Horiek baliatuz informazio sentikorrera sarbidea lor liteke, kodea injektatu edo eskuratu behar ez diren pribilegioak eskuratu.

Konponbidea:

- Liferay Portal 7.1 CE GA4 (7.1.3) edo berriagora eguneratzea.

Xehetasuna:

Larritasun kritikoko ahultasuna honakoa da:

- Kaltetutako produktua ahula da Server Side Request Forgery-ren (SSRF) aurrean, DDM REST datu hornitzailearen bidez. Hori baliatuz erasotzaile batek informazio konfidentzialera sarbidea lor lezake.

Gainerako ahultasunak, larritasun altukoak, honakoak dira:

- Pasahitzen hash-ak eta pasahitzaren oroitarazpenaren erantzunak erregistroetan ager daitezke datu basean akats bat gertatzen bada.
- Hainbat XSS ahultasun baliatuz, urruneko erasotzaile batek web script-ak edo HTML arbitrarioak injekta litzake orrialde batean.
- Direktorio jauzi erako ahultasuna inkesten atalean.
- Baimen batzuk aurrez hautatuta egon daitezke. Ondorioz erabiltzaile batzuk behar ez diren baimenak jaso ditzakete nahi gabe.
- Baimen aniztunak jaulkitzeak eragin lezake erabiltzaileek baimenik gabeko ekintzak egin ahal izatea.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Cisco-ren Data Center Network Manager-en

Argitalpen data: 2019/06/27

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco Data Center Network Manager (DCNM), 11.1 (1) software bertsioa baino lehenagokoak.

Azalpena:

Pedro Ribeiro segurtasun ikertzaile independenteak, ahultasunen berri emateko iDefense programaren bidez, larritasun kritikoko bi ahultasun eta larritasun altuko beste ahultasun bat aurkitu ditu. Autentifikaziorik gabeko urruneko erasotzaile batek fitxategi arbitrarioak igo litzake, autentifikazioa saihestu, administratzaile pribilegioekin ekintza arbitrarioak egin edo kaltetutako gailuko informazio sentikorrera sarbidea lortu.

Konponbidea:

- Data Center Network Manager 11.2(1) bertsiora edo geroagoko batera eguneratzea.

Xehetasuna:

- Larritasun kritikoko ahultasun baten jatorria saioaren kudeaketa okerra da. Autentifikaziorik gabeko urruneko erasotzaile batek bereziki sortutako HTTP eskaera bat egin lezake, gailurako sarbidea lortzeko administratzaile pribilegioekin. Ahultasun horretarako CVE-2019-1619 identifikatzailea erabili da.
- Larritasun kritikoko beste ahultasunaren jatorria baimenen ezarpen oker batzuk dira. Autentifikaziorik gabeko urruneko erasotzaile batek bereziki sortutako datuak bidal litzake fitxategiak aldatzeko eta kode arbitrarioa exekutatzeko root pribilegioekin. Ahultasun horretarako CVE-2019-1620 identifikatzailea erabili da.
- Larritasun altuko ahultasunaren jatorria baimenen ezarpen oker batzuk dira. Autentifikaziorik gabeko urruneko erasotzaile bat kudeaketaren web interfazera konekta liteke eta horrela fitxategi arbitrarioak deskargatu gailutik. Ahultasun horretarako CVE-2019-1621 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun Dell EMCren Unity familian

Argitalpen data: 2019/06/28

Garrantzia: Handia

Kaltetutako baliabideak:

- Dell EMC Unity Operating Environment (OE), 5.0.0.0.5.116 baino lehenagoko bertsioak;
- Dell EMC UnityVSA Operating Environment (OE), 5.0.0.0.5.116 baino lehenagoko bertsioak.

Azalpena:

Dell EMC Unity-k hainbat ahultasunen berri eman du, kaltetutako sistema arriskuan jar dezaketenak.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- Dell EMC Unity Operating Environment (OE) 5.0.0.0.5.116 bertsioa;
- Dell EMC UnityVSA Operating Environment (OE) 5.0.0.0.5.116 bertsioa.

Xehetasuna:

- NAS zerbitzariaren kuoten konfigurazioan baimentze desegoki erako ahultasun bat baliatuz, urrunetik autentifikatutako Unisphere Operator batek beste erabiltzaile batzuen kuoten konfigurazioa edita lezake. Ahultasun horretarako CVE-2019-3734 identifikatzailea erreserbatu da.
- Unisphere-ren erabiltzaileen pasahitzak (administratzaile pribilegioak dituen erabiltzailearenak barne) testu lauan gordetzen dira Unity Data Collection paketean (fitxategiak erregistratzen ditu arazoak konpontzeko). Datuak biltzeko paketera sarbidea lukeen autentifikatutako erasotzaile lokal batek agerian utzitako pasahitzak erabil litzake arriskuan jarritako erabiltzailearen pribilegioekin sarbidea lortzeko. Ahultasun horretarako CVE-2019-3741 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioen eskalatzea F5en hainbat produktutan

Argitalpen data: 2019/06/28

Garrantzia: Handia

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), honako bertsioak:
  - 15.0.0
  - 14.0.0 bertsiotik 14.1.0 bertsiora bitartekoak
  - 13.0.0 bertsiotik 13.1.1 bertsiora bitartekoak
  - 12.1.0 bertsiotik 12.1.4 bertsiora bitartekoak
  - 11.5.2 bertsiotik 11.6.4 bertsiora bitartekoak
- Enterprise Manager 3.1.1 bertsioa
- BIG-IQ Centralized Management honako bertsioak:
  - 6.0.0 bertsiotik 6.1.0 bertsiora bitartekoak
  - 5.1.0 bertsiotik 5.4.0 bertsiora bitartekoak
- F5 iWorkflow 2.3.0 bertsioa

Azalpena:

ING Tech Poland-eko Łukasz Juszczyk eta Robert Podsiadło ikertzaileek kritikotasun altuko ahultasun bat aurkitu dute F5en hainbat produktutan. Autentifikaziorik gabeko erasotzaile batek pribilegioen eskalatzea egin lezake.

Konponbidea:

Oraindik ez da eguneraketarik argitaratu ahultasun hori konpontzeko. Arintze neurri modura, F5ek gomendatzen du "Resource Administrator" rolari lotutako erabiltzaile kontu guztiei TMOS Shell-erako (tmsh) sarbidea desgaitzea.

Xehetasuna:

Ahultasunaren jatorria TMOS Shell (tmsh) terminalean dagoen akats bat da. Autentifikaziorik gabeko erasotzaile batek, fitxategiak kargatzeko aukera balu, pribilegioen eskalatzea egin lezake eta terminal bat lortu root pribilegioekin. Ahultasun horretarako CVE-2019-6642 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna