2018ko Irailaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun HPren produktuetan

Argitalpen data: 2018/09/05

Garrantzia: Handia

Kaltetutako baliabideak:

- HPE 3PAR Service Processors - SP-4.4.0.GA-110 (MU7) baino lehenagokoak
- HP ConvergedSystem 700 Virtualization 2.0 VMware Kit - SWFW Compatibility Matrix August 2018 baino lehenagokoak
- VMware Solution Kit-erako HP ConvergedSystem 700x - SWFW Compatibility Matrix August 2018 baino lehenagokoak
- HP ConvergedSystem 700x v1.1 VMware Kit - SWFW Compatibility Matrix August 2018 baino lehenagokoak

Azalpena:

HPEk segurtasun buletin bat argitaratu du eta bertan 5 ahultasunen berri ematen du, 3 larritasun altukoak eta 2 larritasun ertainekoak. HPE ConvergedSystem 700 sistemetan instalatutako HPE 3PAR prozesagailuen hainbat bertsiori eragiten diete.

Konponbidea:

SP-4.4.0.GA-110 (MU7) bertsiora eguneratzea. Aurreko eguneraketak eskatzen du 3PAR OS egotea 3.2.2MU6 edo goragoko bertsio batean. Xehetasunak eta jarraibideak hemen aurki daitezke:

https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03884en_us

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunak balia litzake ondoko ekintzak egiteko:

- Direktorio jauzia
- Informazio pribilegiatuaren zabalkundea
- Sarbidearen murrizpenari ihes egitea
- Kodearen exekuzioa
- Cross-Site Request Forgery (CSRF)

Ohartarazpen honetan azaldutako ahultasunetarako ondoko identifikatzaileak erreserbatu dira: CVE-2018-7095, CVE-2018-7096, CVE-2018-7097, CVE-2018-7098 eta CVE-2018-7099.

Etiketak: Eguneraketa, HP, Ahultasuna

Ahultasuna IBM WebSphere Application Server-en

Argitalpen data: 2018/09/06

Garrantzia: Handia

Kaltetutako baliabideak:

- WebSphere Application Server bertsio hauek: 7.0, 8.0 eta 8.5.5

Azalpena:

Larritasun altuko ahultasun bat identifikatu da, eta hori baliatuz kaltetutako produktuetan identitatearen ordezpena (*spoofing*) lor liteke.

Konponbidea:

Gomendatutako konponbidea honakoa da: ahalik eta azkarren ezartzea kaltetutako produktu bakoitzerako APAR (*Authorized Program Analysis Report*) PI99402ak dituen IFIX, *Fixpack* edo PTF.

WebSphere Application Server traditional eta WebSphere Application Server Hypervisor Edition-erako:

- 8.5.0.0tik 8.5.5.14ra bitarteko bertsioetarako, Java SE 6 erabiltzen denean, bi aukera daude:
  - IFIXek eskatzen duten *Fixpack*-en gutxieneko mailara eguneratzea eta ondoren *Interim Fix* PI99402 ezartzea.
  - *Fixpack* 8.5.15 edo ondorengoa aplikatzea (2019ko lehen hiru hilekorako eskuragarri izatea espero da).
- 8.0.0.0tik 8.0.0.15era bitarteko bertsioetarako eta 7.0.0.0tik 7.0.0.45era bitarteko bertsioetarako:
  - IFIXek eskatzen duten *Fixpack*-en gutxieneko mailara eguneratzea eta ondoren *Interim Fix* PI99402 ezartzea.

Xehetasuna:

- Java SE 6 erabiltzen denean *Form Login* erabiliz WebSphere Application Server softwareak daukan ahultasun bat baliatuz, erasotzaile batek identitatearen ordezpena (*spoofing*) egitea lor lezake. Horrelakorik ez da gertatzen Java SEren beste bertsio batzuk erabiltzen direnean. Ahultasun horretarako CVE-2018-1695 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2018/09/06

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- RV110W Wireless-N VPN Firewall, bertsio guztiak
- RV130W Wireless-N Multifunction VPN Router, bertsio guztiak
- RV215W Wireless-N VPN Router, bertsio guztiak
- Servicio Cisco Umbrella
- Cisco Webex Meetings Suite (WBS31), (WBS32) eta (WBS33)
- Cisco Webex Meetings
- Cisco Webex Meetings Server
- Cisco Webex Teams, 20180417-150803 baino lehenagoko bertsiodunak
- Cisco Umbrella ERC, 2.1.127 baino lehenagoko bertsiodunak
- Cisco Umbrella Roaming Module, 4.6.1098 baino lehenagoko bertsiodunak
- vEdge 100 serieko routerrak, 18.3.0 baino lehenagoko bertsiodunak
- vEdge 1000 serieko routerrak, 18.3.0 baino lehenagoko bertsiodunak
- vEdge 2000 serieko routerrak, 18.3.0 baino lehenagoko bertsiodunak
- vEdge 5000 serieko routerrak, 18.3.0 baino lehenagoko bertsiodunak
- vManage Network Management System, 18.3.0 baino lehenagoko bertsiodunak
- vEdge Cloud Router Platform, 18.3.0 baino lehenagoko bertsiodunak
- vSmart Controller Software, 18.3.0 baino lehenagoko bertsiodunak
- vBond Orchestrator Software, 18.3.0 baino lehenagoko bertsiodunak
- Cisco Prime Access Registrar, bertsio guztiak, eta Cisco Prime Access Registrar Jumpstar, 7.3.0.4 eta 8.0.1.1 baino lehenagoko bertsioak
- C serieko UCS zerbitzariak, Cisco IMCren honako softwarea exekutatzen dutenak: 2.0 bertsioa, 3.0 bertsioa baldin eta 3.0 (4d) bertsioa baino lehenagokoa bada, edo 3.1 bertsioa baldin eta 3.1 (3a) bertsioa baino lehenagokoa bada
- E serieko UCS zerbitzariak, Cisco IMC softwarearen 3.2 (6) bertsioa baino lehenagokoa exekutatzen dutenak
- 5000 serieko sare sistema enpresarialaren (ENCS) plataformak, Cisco IMC softwarearen 3.2 (6) bertsioa baino lehenagokoa exekutatzen dutenak
- Cisco Data Center Network Manager, 11.0 (1) baino lehenagoko bertsiodunak
- Cisco Webex Player
- Cisco Tetration Analytics
- Cisco Packaged Contact Center Enterprise
- Cisco Prime Collaboration Assurance
- Cisco Network Services Orchestrator (NSO)
- Cisco Enterprise NFV Infrastructure Software (NFVIS)
- Cisco Meeting Server
- Cisco Email Security Appliance (ESA)
- Cisco Cloud Services Platform 2100
- Cisco Secure Access Control Server, 5.8 (10) baino lehenagoko bertsiodunak

Azalpena:

Ciscok bere hainbat produkturi buruzko 29 ahultasun argitaratu ditu, horietatik 2 larritasun kritikokoak, 13 larritasun altukoak eta 14 larritasun ertainekoak.

Konponbidea:

RV110W Wireless-N VPN Firewall eta RV215W Wireless-N VPN Router produktuen kasuan, Ciscok ez du argitaratuko ahultasun horiek konpontzeko firmware eguneraketarik.

Ciscok erabiltzaileen eskura jarri ditu hainbat eguneraketa, kaltetutako produktuaren arabera. Lotura honetan eskura daitezke:

- Software Ciscoren deskarga panela

Xehetasuna:

Larritasun kritikoa duten ahultasunak honakoak dira:

- Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router eta Cisco RV215W Wireless-N VPN Router-en web administrazioko interfazeak duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek zerbitzuaren ukapena eragin lezake edo kode arbitrarioa exekutatu. Ahultasun horren arrazoia web administrazioko interfazearen barnean erabiltzaile gonbidatuaren funtzioan erabiltzaileak emandako sarrerako mugen murrizpen okerrak dira. Gailuak arriskuan egoten dira web administrazioaren interfazearen erabiltzaile gonbidatua gaituta dagoenean soilik. Ahultasun horretarako CVE-2018-0423 identifikatzailea erreserbatu da.
- Ciscoren Umbrella APIak duen ahultasun bat baliatuz, urruneko erasotzaile autentifikatu batek bere erakundean edo beste erakunde batzuetan datuak ikus eta alda litzake. Horren arrazoia da API interfazerako autentifikazioaren konfigurazio ez aski bat. Ahultasun horretarako CVE-2018-0435 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2018-0422, CVE-2018-0436, CVE-2018-0437 CVE-2018-0438, CVE-2018-0434, CVE-2018-0433, CVE-2018-0432, CVE-2018-0426, CVE-2018-0424, CVE-2018-0425, CVE-2018-0421, CVE-2018-0430, CVE-2018-0431, CVE-2018-0440 CVE-2018-0457, CVE-2018-0452, CVE-2018-0451, CVE-2018-0444, CVE-2018-0445, CVE-2018-

0458, CVE-2018-0463, CVE-2018-0459, CVE-2018-0447, CVE-2018-0460, CVE-2018-0462, CVE-2018-0439, CVE-2018-0450, CVE-2018-0454 eta CVE-2018-0414.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Kodearen urruneko exekuzioa IBMren WebSphere Application Server-en

Argitalpen data: 2018/09/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IBM WebSphere Appliaction, 9.0, 8.5, 8.0 eta 7.0 bertsioak

Azalpena:

IBMk larritasun kritikoko ahultasun bat argitaratu du bere WebSphere Application produktuei eragiten diena eta urrunetik kodea exekutatzea ahalbidetu lezakeena.

Konponbidea:

Gomendatutako konponbidea honakoa da: ahalik eta azkarren ezartzea kaltetutako produktu bakoitzerako APAR (*Authorized Program Analysis Report*) PI95973ak dituen IFIX, *Fixpack* edo PTF.

WebSphere Application Server traditional eta WebSphere Application Server Hypervisor Edition-erako:

- 9.0.0.0tik 9.0.0.9ra bitarteko bertsioetarako bi aukera daude:
  - IFIXek eskatzen duten *Fixpack*-en gutxieneko mailara eguneratzea eta ondoren *Interim Fix* PI95973 ezartzea
  - *Fixpack* 9.0.0.10 edo ondorengoa aplikatzea (2018ko azken hiruhilekorako eskuragarri izatea espero da).
- 8.5.0.0tik 8.5.5.14ra bitarteko bertsioetarako bi aukera daude:
  - IFIXek eskatzen duten *Fixpack*-en gutxieneko mailara eguneratzea eta ondoren *Interim Fix* PI95973 ezartzea
  - *Fixpack* 8.5.5.15 edo ondorengoa aplikatzea (2019ko lehen hiruhilekorako eskuragarri izatea espero da).
- 8.0.0.0tik 8.0.0.15era bitarteko bertsioetarako:
  - IFIXek eskatzen duten *Fixpack*-en gutxieneko mailara eguneratzea eta ondoren *Interim Fix* PI95973 ezartzea
- 7.0.0.0tik 7.0.0.45era bitarteko bertsioetarako:
  - IFIXek eskatzen duten *Fixpack*-en gutxieneko mailara eguneratzea eta ondoren *Interim Fix* PI95973 ezartzea

Xehetasuna:

- Ahultasun hau baliatuz urruneko erasotzaileek Java kode arbitrarioa exekuta lezakete SOAP konektorearen bidez, iturri ez-fidagarrietako objektu serializatu batekin. Ahultasun horretarako CVE-2018-1567 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Pribilegioen eskalatze erako ahultasuna ProtonVPN bezeroan

Argitalpen data: 2018/09/10

Garrantzia: Handia

Kaltetutako baliabideak:

- VPN ProtonVPN 1.5.1en bezeroa

Azalpena:

ProtonVPN 6.14.28.0ren VPN bezeroaren konexio funtzionaltasunean balia daitekeen kodearen exekuzioko ahultasuna dago. Bereziki diseinatutako OpenVPN konfigurazio fitxategi batek pribilegioen eskalatzea eragin lezake eta horrek komando arbitrarioen exekuzioa ahalbidetu lezake sistemaren pribilegioekin.

Konponbidea:

Ahultasun hau uztailean eman zuen argitara ekipoak, eta partxea irailaren 3ko eguneraketan sartu da. Bezeroei aholkatzen zaie VPNa oraingo bertsiora eguneratzea.

Xehetasuna:

Cisco Taloseko Paul Rascagneres ikertzaileak aurkitu duenez, OpenVPNren konfigurazio fitxategia aldatzen bada eta *up* parametroa gehitzen bada eta ondoren edozein programaren exekuzio-bidea ere, programa sistemaren pribilegioekin exekutatuko da. Ahultasun horretarako CVE-2018-4010 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Pribilegioen eskalatze erako ahultasuna NordVPN bezeroan

Argitalpen data: 2018/09/10

Garrantzia: Handia

Kaltetutako baliabideak:

- VPN NordVPN 6.14.28.0ren bezeroa

Azalpena:

NordVPN 6.14.28.0ren VPN bezeroaren konexio funtzionaltasunean balia daitekeen kodearen exekuzioko ahultasuna dago. Bereziki diseinatutako OpenVPN konfigurazio fitxategi batek pribilegioen eskalatzea eragin lezake, eta horrek komando arbitrarioen exekuzioa ahalbidetu lezake sistemaren pribilegioekin.

Konponbidea:

Abuztuaren 8ko VPN bezeroaren eguneraketan partxe bat barneratu da. Bezeroei aholkatzen zaie VPNa oraingo bertsiora eguneratzea.

Xehetasuna:

Cisco Taloseko Paul Rascagneres ikertzaileak aurkitu duenez, OpenVPNren konfigurazio fitxategia aldatzen bada eta *up* parametroa gehitzen bada eta ondoren edozein programaren exekuzio-bidea ere, programa sistemaren pribilegioekin exekutatuko da. Ahultasun horretarako CVE-2018-3952 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun HPE produktuetan

Argitalpen data: 2018/09/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Intelligent Management Center

Azalpena:

Sztivi ikertzaileak larritasun kritikoko 9 ahultasun aurkitu ditu HPE produktuetan. Horiek baliatuz autentifikaziorik gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

Oraingoz ez dago inolako eguneraketarik ahultasun horiek konpontzeko. Arintze neurri modura, konfiantzako makinekin zerbitzuarekiko interakzioa murriztea gomendatzen da, adibidez suebakiekin eta zerrenda zuriekin.

Xehetasuna:

- Erasotzaile batek ahultasunak balia litzake kode arbitrarioa exekutatzeko SYSTEM testuinguruan, ondokoaren ondorioz:
  - Erabiltzaileak dbman zerbitzuan, TCP 2810 ataka portuan (lehenetsita), emandako sarrera datuen egiaztatze desegokia.
  - TCP 2810 entzuteko atakan, dbman zerbitzuan opcode 10010ren eskaeren maneiua, erabiltzaileak kontrolatutako datuak dituzten fitxategietan idazketa arbitrarioa ahalbidetzen duena.
  - dealInodeNotifyMsg metodoari emandako erabiltzaile izenaren parametroaren egiaztatze desegokia, luzera finkoko piletan oinarritutako buffer batera kopiatuak izan baino lehen.
  - Mezu enkriptatuen deszifratuaren barnean erabiltzaileak emandako datuen luzeraren araketa desegokia, luzera finkoko piletan oinarritutako buffer batera kopiatuak izan baino lehen.
  - dealInodeOfflineMsg mezuaren prozesamenduak ez du modu egokian balioztatzen erabiltzaileak emandako datuen luzera, luzera finkoko piletan oinarritutako buffer batera kopiatuak izan baino lehen.

Etiketak: 0day, HP, Ahultasuna

2018ko iraileko Microsoften segurtasun buletina

Argitalpen data: 2018/09/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office and Microsoft Office Services and Web Apps
- ChakraCore
- Adobe Flash Player
- . NET Framework
- Microsoft.Data.OData
- ASP.NET

Azalpena:

Segurtasun eguneraketen inguruko hileroko Microsoft argitalpenean 60 ahultasun jaso dira oraingoan; 17 kritiko gisa sailkatu dira eta 43 garrantzitsu gisa. Gainerakoak larritasun ertain edo baxukoak dira.

Konponbidea:

Dagozkien segurtasun eguneraketak instalatzea. Eguneraketen instalazio informazioari buruzko orrian hori egiteko metodo ezberdinei buruzko informazioa dago.

Xehetasuna:

Argitaratutako ahultasun motak ondokoak dira:

- Pribilegioen igoera.

- Zerbitzua ukatzea.
- Kodearen urrutiko exekuzioa.
- Informazioa ezagutaraztea.
- Ordezpena.
- Segurtasunari ihes egitea.

Etiketak: Eguneraketa, Microsoft, Nabigatzailea, Sistema Eragilea, Ahultasuna

---

SAPen segurtasun eguneraketa 2018ko irailean

Argitalpen data: 2018/09/12

Garrantzia: Handia

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa
- SAP Business One, 9.2 eta 9.3 bertsioak
- SAP NetWeaver BI, 7.30,7.31,7.40,7.41 eta 7.50 bertsioak
- SAP HANA, 1.0 eta 2.0 bertsioak
- SAP WebDynpro, 7.20, 7.30, 7.31, 7.40, 7.50 bertsioak
- SAP NetWeaver AS Java, 7.10etik 7.11, 7.20, 7.30, 7.31, 7.40, 7.50era bitarteko bertsioak
- SAP Hybris Commerce, 6.* bertsioak
- SAP Plant Connectivity, 15.0 bertsioa
- SAP Adaptive Server Enterprise, 16.0 bertsioa
- SAP HCM Fiori "People Profile" (GBX01HR), 6.0 bertsioa
- SAP Mobile Platform, 3.0 bertsioa
- SAP Enterprise Financial Services, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0 bertsioa
- SAP Business One Android application, 1.2 bertsioa

Azalpena:

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

Konponbidea:

SAPen laguntzarako webgunea bisitatu eta fabrikatzaileak adierazten duen moduan beharrezkoak diren eguneraketa edo partxeak instalatzea.

Xehetasuna:

SAPek segurtasun partxeei buruz argitaratzen duen hileroko komunikatuan 14 segurtasun ohar eman ditu ezagutzera. Horietatik ohar 1 lehenagotik argitaratutako segurtasun ohar bati dagokion eguneraketa da, beste 3 larritasun altukoak dira, 9 larritasun ertainekoak eta beste 1 larritasun baxukoa.

Argitaratutako ahultasun motak ondokoak dira:

- Zerbitzuaren ukazioko ahultasun bat
- Informazio zabalkundeko 3 ahultasun
- Baimenaren egiaztapen gabeziako 3 ahultasun
- Cross-Site Scripting erako 2 ahultasun
- XMLren balioztatze okerreko 2 ahultasun
- Beste tipologia batzuetako 3 ahultasun

Ahultasun garrantzitsuenak ondokoak dira:

· SAP Business ONEk eta SAP HANAk duten informazioaren zabalkunde erako ahultasuna baliatuz, erasotzaile batek informazio gehigarria zabal lezake (sistemaren datuak, depurazio informazioa eta abar), eta horrek sistemari buruzko ezagupenak lortzen lagundu lezake beste eraso batzuk prestatzeko. Horren ondorioz informazioaren zabalkundea, pribilegioen eskalatzea eta beste eraso batzuk gerta litezke. CVE-2018-2458 kodea esleitu zaio ahultasun horri.

· Erasotzaile batek SAP BEx Web Java Runtime Export Web Service-k duen XMLren balioztatze okerreko ahultasuna balia lezake bereziki diseinatutako eta baimendu gabeko XML eskaerak bidaltzeko, XML analizatzaileak prozesatuko lituzkeenak. Horrela erasotzaileak Sistema Eragileko fitxategien sistemara baimendu gabeko sarbidea lortuko luke. CVE-2018-2462 kodea esleitu zaio ahultasun horri.

· SAP ECC Sales Supportek duen baimenaren egiaztapen gabeziako ahultasun bat baliatuz, erasotzaile batek zerbitzu batera sarbidea lor lezake baimenaren beharrik gabe eta sarbide mugatuko zerbitzu funtzioak erabili behar izan gabe. Horren ondorioz informazioaren zabalkundea, pribilegioen eskalatzea eta beste eraso batzuk gerta litezke.

Etiketak: Eguneraketa, SAP, Ahultasuna

Hainbat ahultasun Intel produktuetan

Argitalpen data: 2018/09/12

Garrantzia: Handia

Kaltetutako baliabideak:

- Intel® Data Migration Software, v3.1 eta lehenagoko bertsioak
- Intel® OpenVINO™ Toolkit for Windows, v2018.1.265 eta lehenagoko bertsioak
- Intel® IoT Developers Kit, 4.0 eta lehenagoko bertsioak
- Intel® NUC Kit, hainbat modelo
- Intel® Compute Card, hainbat modelo
- Intel® Compute Stick, hainbat modelo
- Intel® Centrino® Wireless-N, hainbat modelo
- Intel® Centrino® Advanced-N, hainbat modelo
- Intel® Distribution for Python 2018, 2018ko abuztuaren 6a baino lehen deskargatutako bertsioak
- Intel® Extreme Tuning Utility, 6.4.1.23 bertsioa baino lehenagokoak

- Intel® Driver & Support Assistant, 3.5.0.1 bertsioa baino lehenagokoak
- Intel® Computing Improvement Program, 2.2.0.03942 bertsioa baino lehenagokoak
- Intel-SA-00086 Detection Tool, 1.2.7.0 bertsioa baino lehenagokoak
- Intel® CSME, 11.0tik 11.8.50era bitarteko bertsioak; 11.10tik 11.11.50era bitartekoak; 11.20tik 11.21.51era bitartekoak, Intel® Server Platform Services 4.0 firmware bertsioa (soilik Purley eta Bakerville) eta Intel® TXE, 3.0tik 3.1.50era bitarteko bertsioak.
- Intel® CSME erabiltzen duten sistemak, firmwarearen 11.0 bertsioa baino lehenagokoa dutenak / Intel® Server Platform Services 4.0 / TXE 3.0, edo firmwarearen 11.8.55, 11.11.55 edo 11.21.55 bertsioak erabiltzen dituztenak / Intel® Server Platform Services 5.0 eta goragokoak / TXE 3.1.55 edo goragokoak ez daude ahultasun honek kaltetuta.
- Intel® CSME, hainbat bertsio
- Intel® ME, hainbat bertsio
- Intel® Trusted Execution Engine (TXE), hainbat bertsio
- Intel® Data Center manager, 5.1 baino lehenagoko bertsioak
- Intel® Server Board, hainbat bertsio
- Intel® Server Board S2600BP, S2600WF eta S2600ST

Azalpena:

Intelek 16 segurtasun ohartarazpen argitaratu ditu produktuen bere segurtasun zentroan, 1 larritasun kritikokoa, 7 larritasun altukoak eta 8 larritasun ertainekoak.

Konponbidea:

Produktuaren azken bertsiora eguneratzea hemen: https://downloadcenter.intel.com/.

Xehetasuna:

Asmo gaiztoko erabiltzaile batek aipatutako ahultasunak baliatuko balitu, kaltetutako produktuetan ondoko ekintzak egin litzake:

- Pribilegioen eskalatzea
- Kodea exekutatzea beste pribilegio batzuekin
- Kode arbitrarioa exekutatzea
- Informazioa ezagutaraztea
- Zerbitzua ukatzea

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Moodle-n

Argitalpen data: 2018/09/17

Garrantzia: Handia

Kaltetutako baliabideak:

Ondoko bertsioak izan dira kaltetuak, ahultasunen arabera:

- MSA-18-0019: 3.5etik 3.5.1era bitartekoak, 3.4tik 3.4.4ra bitartekoak, 3.3tik 3.3.7ra bitartekoak, eta zerbitzurik gabeko lehenagoko bertsioak.
- MSA-18-0018: 3.5etik 3.5.1era bitartekoak, 3.4tik 3.4.4ra bitartekoak, 3.3tik 3.3.7ra bitartekoak, 3.1etik 3.1.13ra bitartekoak eta zerbitzurik gabeko lehenagoko bertsioak.
- MSA-18-0017: 3.5etik 3.5.1era bitartekoak, 3.4tik 3.4.4ra bitartekoak, 3.1etik 3.1.13ra bitartekoak, eta zerbitzurik gabeko lehenagoko bertsioak.

Azalpena:

Moodlen 3 ahultasun aurkitu dira, bat kritikotasun altukoa eta beste bi kritikotasun baxukoak. Ahultasun horiek XSS islatu bat (edo zeharkakoa) edo PHP kodearen injekzioa eta exekuzioa eragin lezakete. Gainera, hirugarrenen liburutegi bat eguneratu da zuhurtziazko neurri modura.

Konponbidea:

Erabiltzaileen eskura jarri dira ondoko eguneraketak, ahultasun bakoitzaren arabera:

- MSA-18-0019: 3.5.2, 3.4.5 eta 3.3.8.
- MSA-18-0018 eta MSA-18-0017: 3.5.2, 3.4.5, 3.3.8 eta 3.1.14.

Xehetasuna:

Kritikotasun altuko ahultasuna ondokoa da:

- *Drag and drop into text* metodoarekin heredatutako frogazko galderak inportatzean, erasotzaile batek PHP kodea injekta eta exekuta lezake inportatutako galderetan, bai nahita edo bai iturri ez fidagarri batetik galderak inportatuz.

Ahultasun horietarako honako identifikatzaileak erreserbatu dira: CVE-2018-14631 (MSA-18-0019), CVE-2018-1999022 (MSA-18-0018) eta CVE-2018-14630 (MSA-18-0017).

Etiketak: Eguneraketa, Edukien kudeatzailea, Ahultasuna

Ahultasuna F5en BIG-IP ASM-n

Argitalpen data: 2018/09/19

Garrantzia: Ertaina

Kaltetutako baliabideak:

- BIG-IP ASM, 12.1.2 eta 12.1.3.6 bitarteko bertsioak

Azalpena:

F5ek BIG-IP ASMri eragiten dion ahultasun bat aurkitu du. Hori dela eta, eraso sinadurak aplikatzeari utz diezaioke, sinadura berri bat barneratzen duen segurtasun politika bat aktibatu ondoren.

Konponbidea:

F5ek eguneraketa bat argitaratu du 12.1.3.7 bertsiora. Gainerako segurtasun politikak eguneratzea ere gomendatzen du, sinaduren bildumaren ID berriari erreferentzia egitearren.

Xehetasuna:

Arazoa sortzen da ondoko baldintzak betetzen direnean:

- BIG-IP ASM sistemak 12.1.2 eta 12.1.3.6 bertsioak eguneratzea.
- BIG-IP ASM sisteman hainbat segurtasun politika konfiguratuta izatea.
- Segurtasun politiketako batek beste politika batzuetan jasota ez dagoen eraso-sinadura berri bat izatea.
- Sinadura berria barneratuta daukan segurtasun politika aktibatzea.

Segurtasun politika aktibatzen denean, sistemak oinarrizko sinaduren bilduma freskatzen du gehitutako ID batekin. Arazo hori gertatzen denean, soilik berriki aktibatutako segurtasun politika eguneratzen da sinaduren bildumaren ID berriari erreferentzia egiteko.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Cisco Webex Network Recording Player-en

Argitalpen data: 2018/09/20

Garrantzia: Handia

Kaltetutako baliabideak:

- Cisco Webex Meetings Suite (WBS32) - Webex Network Recording Player, WBS32.15.10 baino lehenagoko bertsioak
- Cisco Webex Meetings Suite (WBS33) - Webex Network Recording Player, WBS33.3 baino lehenagoko bertsioak
- Cisco Webex Meetings Online - Webex Network Recording Player, 1.3.37 baino lehenagoko bertsioak
- Cisco Webex Meetings Server - Webex Network Recording Player, 3.0MR2 baino lehenagoko bertsioak

Azalpena:

Ciscok segurtasun ohartarazpen bat argitaratu du larritasun altuko 3 ahultasunen berri emanez. Horiek baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake kaltetutako sistemetan.

Konponbidea:

Ohartarazpen honetan azaltzen diren ahultasunak konpondu egiten dituzte produktuen bertsio hauek:

- Cisco Webex Meetings Suite (WBS32) - Cisco Webex Network Recording Player, WBS32.15.10 eta ondorengo bertsioak
- Cisco Webex Meetings Suite (WBS33) - Cisco Webex Network Recording Player, WBS33.3 eta ondorengo bertsioak
- Cisco Webex Meetings Online - Webex Network Recording Player, 1.3.37 eta ondorengo bertsioak
- Cisco Webex Meetings Server - Webex Network Recording Player, 3.0MR2 eta ondorengo bertsioak

ARF erreproduzitzailearen azken bertsioak hemen eskura daitezke:

http://www.webex.com/play-webex-recording.html

Xehetasuna:

Erabiltzaile batek lotura batean klika dezan edo email gaizto bateko fitxategia ireki dezan lortuz gero, zibergaizkileak kode arbitrarioa exekutatzea lor lezake kaltetutako sistemetan. Ahultasun horietarako CVE-2018-15414, CVE-2018-15421 eta CVE-2018-15422 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun IBMren Db2-n

Argitalpen data: 2018/09/21

Garrantzia: Handia

Kaltetutako baliabideak:

IBM Db2ren bertsio hauek:

- V9.7.
- V10.1.
- V10.5.
- V11.1.

Azalpena:

IBMk kritikotasun altuko 3 ahultasun aurkitu ditu Db2-n. Horien bitartez, erasotzaile lokal batek pribilegioen igoera lor lezake eta bufferraren gainezkatzea eragin kode arbitrarioa exekutatuz.

Db2ren beste ahultasun batzuk ere argitaratu ditu, kritikotasun ertain edo baxukoak. Erreferentzien atalean informazio gehiago aurki daiteke.

Konponbidea:

IBMk erabiltzaileen eskura jarri ditu ahultasunak konpontzen dituzten segurtasun eguneraketak, kaltetutako bertsio bakoitzaren arabera.

Ondoko loturan eskura daitezke:

Fix Central

Xehetasuna:

- db2licm tresnak duen bufferraren gainezkatze erako ahultasun batek kodea arbitrarioki exekutatzea ahalbidetu lezake. Ahultasun horretarako CVE-2018-1710 identifikatzailea erreserbatu da.
- IBM Db2ren lan administratiboen planifikatzaileak duen ahultasun bat baliatuz, erabiltzaile lokal batek pribilegioak lor litzake, dauden lanen zutabeak aldatzen uzten baitu. Ahultasun horretarako CVE-2018-1711 identifikatzailea erreserbatu da.
- Db2k erabiltzen duen IBM Spectrum Scale-ri eragiten dion GSKit-en ahultasun bat baliatuz, erasotzaile batek Spectrum Scale daemon-en kontrola har lezake, Spectrum Scales-en fitxategien sisteman fitxategietara sar liteke eta horiek aldatu, eta seguruenik nodoan administratzaile pribilegioak lortu. Ahultasun horretarako CVE-2018-1431 identifikatzailea erabili da.

Larritasun ertain edo baxuko ahultasunetarako honako identifikatzaileak erabili dira: CVE-2016-0705, CVE-2017-3732, CVE-2018-1447.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun HPE produktuetan

Argitalpen data: 2018/09/21

Garrantzia: Handia

Kaltetutako baliabideak:

- HP XP7 Automation Director Software, 8.5.2-02tik 8.6.1-00 bertsioa baino lehenagokora.
- HPE XP7 Automation Director Software, 8.5.2-02tik 8.6.1-00 bertsioa baino lehenagokora ondoko modeloen kasuan: 1TB 101-250TB LTU, 1TB 251-500TB LTU, 1TB Enterprise LTU, 1TB Over 500TB LTU, 1TB-day Meter LTU, Base LTU eta Unlimited LTU.
- HPE XP P9000 Command View Advanced Edition Software-ren lizentzia guztiak.
- HPE XP7 Command View Advanced Edition Suite guztiak.
- HPE 3PAR Service Processors - SP-4.4.0.GA-110 (MU7) baino lehenagokoak.
- HP ConvergedSystem 700 Virtualization 2.0 VMware Kit - SWFW Compatibility Matrix 2017ko azarokoa baino lehenagokoak.
- HP ConvergedSystem 700x for VMware Solution Kit - SWFW Compatibility Matrix 2017ko azarokoa baino lehenagokoak.
- HP ConvergedSystem 700x v1.1 VMware Kit - SWFW Compatibility Matrix 2017ko azarokoa baino lehenagokoak.
- HPE enhanced Internet Usage Manager (eIUM) 9.0 FP01 - 9.0 FP01 bertsioan oinarritutako bezeroaren bertsio espezifikoak barne.

Azalpena:

Hainbat ahultasun aurkitu dira HPEren zenbait produktutan:

- HPE StorageWorks XP7 Automation Director-en autentifikazio lokal eta urrunekoaren *bypass*-a gerta liteke.
- HPE XP P9000 Command View Advanced Edition-en informazio sentikorrera baimen gabeko sarbidea lor liteke, bai modu lokalean eta bai urrunetik.
- HPE Command View Advanced Edition-en murrizpen lokal eta urrunekoaren *bypass*-a eragin liteke.
- HPE Command View Advanced Edition-en JDK erabiliz autentifikazio lokal eta urrunekoaren *bypass*-a eragin liteke.
- HPE ConvergedSystem 700 Solutions-ek hainbat ahultasun ditu HPE 3PAR Service Processor erabiltzean.
- HPE Internet Usage Manager hobetuak fitxategi arbitrarioen urruneko aldaketa eragin lezake.

Konponbidea:

- HPE StorageWorks XP7 Automation Director-en kasuan, AutoDir 8.6.1-00 bertsiora edo berriagoetara eguneratu.
- HPE XP P9000 Command View Advanced Edition-en kasuan, DevMgr 8.6.1-00 eta CM 8.6.1-00 eguneraketak aplikatu (soilik REST API erabiltzen bada, bestela CM desinstalatu).
- HPE Command View Advanced Edition-en kasuan, ondoren zehazten diren bertsioetara edo berriagoetara eguneratu:
  - DevMgr 8.6.0-00: DevMgr 8.4.0-00 edo bertsio berriagoez geroztik, CM ere automatikoki dago DevMgr-rekin batera instalatuta. Ahultasuna konponduta dago DevMgr 8.6.0-00 bertsioan, CM 8.6.0-00 barneratzen duena. Ahultasun hori konpontzeko:
    - DevMgr eta CM eguneratu 8.6.1-00 bertsiora edo berriagoetara.
    - CM funtzionaltasuna ez bada beharrezkoa, CM desinstalatu DevMgr 8.6.0-00 eguneratu ondoren.
  - TSMgr 8.6.0-00
  - RepMgr 8.6.0-00
  - HGLM 8.6.0-00
  - AutoDir 8.6.0-00
  - CM 8.6.1-00: DevMgr 8.4.0-00 edo bertsio berriagoez geroztik, CM ere automatikoki dago DevMgr-rekin batera instalatuta. Ahultasuna konponduta dago DevMgr 8.6.0-00 bertsioan, CM 8.6.0-00 barneratzen duena. Ahultasun hori konpontzeko:
    - DevMgr eta CM eguneratu 8.6.1-00 bertsiora edo berriagoetara.
    - CM funtzionaltasuna ez bada beharrezkoa, CM desinstalatu DevMgr 8.6.0-00 eguneratu ondoren.
- HPE Command View Advanced Edition-en kasuan ahultasunak produktuen etorkizuneko bertsio batean konponduko dira. Behin-behineko konponbide modura, produktu hauek erabiltzen duten JDK aldatu egin daiteke Oracle JDKgatik (8u181 edo goragokoa).
- HPE 3PAR Service Processor erabiltzen duen HPE ConvergedSystem 700 Solutions-en kasuan, *Erreferentziak* atalean zerrendatutako ahultasunaren webgunean adierazitako jarraibideak ezarri.
- HPE Internet Usage Manager hobetuaren kasuan, azken eIUM90FP01XXX.YYYYMMDD-HHMM metatze partxea ezarri behar zaie 9.0 FP01XXX bertsioan oinarritutako instalazio guztiei, non XXX bezeroaren identifikatzailea den.

Xehetasuna:

Asmo gaiztoko erabiltzaile batek aipatutako ahultasunak baliatuko balitu, kaltetutako produktuetan ondoko ekintzak egin litzake:

- HPE StorageWorks XP7 Automation Director (AutoDir) 8.5.2-02tik 8.6.1-00 bertsioa baino lehenagokora bitartekoek biltegiratze sistemako erabiltzailearen autentifikazioaren agerpen motako ahultasuna daukate. Arazo hau batzuetan gertatzen da, zerbitzu txantiloi bat exekutatzean ematen diren baldintza zehatz batzuetan. CVE-2018-7108 identifikatzailea esleitu zaio.
- HPE XP P9000 Command View Advanced Edition (CVAE) produktuek web zerbitzarian ahultasun bat daukate, erabiltzailearen informazioa berreskuratze motakoa, CVAE produktuen barnean joan ohi dena. Software hau balia liteke informazio konfidentzialera baimenik gabeko sarbide lokal eta urrunekoa lortzeko. CVE-2016-9877 identifikatzailea esleitu zaio.
- HPE Command View Advanced Edition-ek (CVAE) sarbide lokal eta urrunekoaren murrizpeneko *bypass* erako ahultasuna dauka. CVE-2017-3736 eta CVE-2017-3738 identifikatzaileak erabili dira.
- HPE Command View Advanced Edition-ek (CVAE) JDK erabiltzean sarbide lokal eta urrunekoaren murrizpeneko *bypass* erako ahultasuna dauka. CVE-2018-2940, CVE-2018-2952 eta CVE-2018-2973 identifikatzaileak erabili dira.
- HPE 3PAR Service Processor erabiltzean HPE ConvergedSystem 700 Solutions-ek dituen ahultasunak lokalki baliatuz ondokoak egin litzake: direktorioak gurutzatu, informazio pribilegiatua zabaldu eta urrunetik sarbidearen murrizpena saihestu, kodea exekutatu eta Cross-Site Request Forgery (CSRF). CVE-2018-7095, CVE-2018-7096, CVE-2018-7097, CVE-2018-7098 eta CVE-2018-7099

identifikatzaileak erabili dira.
- HPE Internet Usage Manager hobetuak (eIUM) fitxategien urruneko aldaketa arbitrario erako ahultasuna dauka. CVE-2018-7109 identifikatzailea esleitu zaio.

Etiketak: Eguneraketa, HP, Ahultasuna

Ahultasuna Cisco Video Surveillance Manager-en

Argitalpen data: 2018/09/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Cisco Video Surveillance, Ciscok aurreinstalatua bertsio hauetan:

- 7.10
- 7.11
- 7.11.1

Ondoko plataforma hauetakoren batean exekutatzen den bitartean:

- CPS-UCSM4-1RU-K9
- CPS-UCSM4-2RU-K9
- KIN-UCSM5-1RU-K9
- KIN-UCSM5-2RU-K9

Azalpena:

Cisco Unified Computing System-en (UCS) plataforma batzuetan exekutatzen denean Cisco Video Surveillance Manager (VSM) softwareak duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek kaltetutako sisteman saioa has lezake *root* kontuaren bidez lehenetsitako kredentzialekin, eta horrela komando arbitrarioak exekuta litzake.

Konponbidea:

Ahultasun hau konpontzeko Ciscok 7.12 bertsiorako eguneraketa bat argitaratu du, bere webgunean eskura daitekeena.

Xehetasuna:

Cisco Unified Computing System-en (UCS) plataforma batzuetan exekutatzen denean Cisco Video Surveillance Manager (VSM) softwareak duen ahultasun bat aurkitu da. Hori baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek kaltetutako sisteman saioa has lezake lehenetsitako kredentzialak dituen *root* kontuaren bidez, eta horrela komando arbitrarioak exekuta litzake.

Ahultasun hau gertatzen da Ciscok ez zuelako *root* kontua desgaitu softwarea aurreinstalatu baino lehen. Kontu horretarako kredentzialak ez daude dokumentatuta modu publikoan. Ahultasun horretarako CVE-2018-15427 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun Netgear produktuetan

Argitalpen data: 2018/09/26

Garrantzia: Handia

Kaltetutako baliabideak:

- D3600, 1.0.0.76 baino lehenagoko bertsioak
- D6000, 1.0.0.76 baino lehenagoko bertsioak
- D1500, 1.0.0.27 baino lehenagoko bertsioak
- D500, 1.0.0.27 baino lehenagoko bertsioak
- D6100, 1.0.0.58 baino lehenagoko bertsioak
- D6200, 1.1.00.30 baino lehenagoko bertsioak
- D6220, 1.0.0.46 baino lehenagoko bertsioak
- D6400, 1.0.0.82 baino lehenagoko bertsioak
- D7000, 1.0.1.68 baino lehenagoko bertsioak
- D7000v2, 1.0.0.51 baino lehenagoko bertsioak
- D7800, 1.0.1.42 baino lehenagoko bertsioak
- D8500, 1.0.3.42 baino lehenagoko bertsioak
- DC112A, 1.0.0.40 baino lehenagoko bertsioak
- DGN2200Bv4, 1.0.0.102 baino lehenagoko bertsioak
- DGN2200v4, 1.0.0.102 baino lehenagoko bertsioak
- JNR1010v2, 1.1.0.54 baino lehenagoko bertsioak
- JR6150, 1.0.1.18 baino lehenagoko bertsioak
- JWNR2010v5, 1.1.0.54 baino lehenagoko bertsioak
- PR2000, 1.0.0.24 baino lehenagoko bertsioak
- R6020, 1.0.0.34 baino lehenagoko bertsioak
- R6050, 1.0.1.18 baino lehenagoko bertsioak
- R6080, 1.0.0.34 baino lehenagoko bertsioak
- R6100, 1.0.1.22 baino lehenagoko bertsioak
- R6120, 1.0.0.42 baino lehenagoko bertsioak
- R6220, 1.1.0.68 baino lehenagoko bertsioak
- R6250, 1.0.4.30 baino lehenagoko bertsioak
- R6300v2, 1.0.4.32 baino lehenagoko bertsioak
- R6400, 1.0.1.44 baino lehenagoko bertsioak
- R6400v2, 1.0.2.60 baino lehenagoko bertsioak
- R6700, 1.0.1.48 baino lehenagoko bertsioak
- R6700v2, 1.2.0.24 baino lehenagoko bertsioak
- R6800, 1.2.0.24 baino lehenagoko bertsioak
- R6900, 1.0.1.48 baino lehenagoko bertsioak

- R6900P, 1.3.1.44 baino lehenagoko bertsioak
- R6900v2, 1.2.0.24 baino lehenagoko bertsioak
- R7000, 1.0.9.34 baino lehenagoko bertsioak
- R7000P, 1.3.1.44 baino lehenagoko bertsioak
- R7100LG, 1.0.0.48 baino lehenagoko bertsioak
- R7300, 1.0.0.68 baino lehenagoko bertsioak
- R7500, 1.0.0.124 baino lehenagoko bertsioak
- R7500v2, 1.0.3.38 baino lehenagoko bertsioak
- R7900, 1.0.2.16 baino lehenagoko bertsioak
- R7900P, 1.4.1.24 baino lehenagoko bertsioak
- R8000, 1.0.4.18 baino lehenagoko bertsioak
- R8000P, 1.4.1.24 baino lehenagoko bertsioak
- R8300, 1.0.2.122 baino lehenagoko bertsioak
- R8500, 1.0.2.122 baino lehenagoko bertsioak
- WN3000RP, 1.0.0.68 baino lehenagoko bertsioak
- WN3000RPv2, 1.0.0.68 baino lehenagoko bertsioak
- WNDR3400v3, 1.0.1.18 baino lehenagoko bertsioak
- WNDR3700v4, 1.0.2.102 baino lehenagoko bertsioak
- WNDR3700v5, 1.1.0.54 baino lehenagoko bertsioak
- WNDR4300v1, 1.0.2.104 baino lehenagoko bertsioak
- WNDR4300v2, 1.0.0.56 baino lehenagoko bertsioak
- WNDR4500v3, 1.0.0.56 baino lehenagoko bertsioak
- WNR1000v4, 1.1.0.54 baino lehenagoko bertsioak
- WNR2020, 1.1.0.54 baino lehenagoko bertsioak
- WNR2050, 1.1.0.54 baino lehenagoko bertsioak
- WNR3500Lv2, 1.2.0.54 baino lehenagoko bertsioak

Azalpena:

Netgear-ek larritasun altuko 2 ahultasun argitaratu ditu, bere router, wifi hedatzaile eta hedapen base batzuei eragiten dietenak.

Konponbidea:

Kaltetutako produktuak firmwarearen azken bertsiora eguneratzea, hemen eskuragarri: https://www.netgear.com/support/.

Xehetasuna:

- Segurtasunaren konfigurazio okerragatiko ahultasuna, D3600 eta D6000 routerrei eragiten diena.
- Informazio sentikorraren zabalkunde erako ahultasuna, kaltetutako gainerako produktuei eragiten diena.

Etiketak: Eguneraketa, Pribatutasuna, Ahultasuna

Hainbat ahultasun Jenkins-en

Argitalpen data: 2018/09/26

Garrantzia: Handia

Kaltetutako baliabideak:

- Arachni Scanner Plugin, 0.9.7 eta lehenagoko bertsioak.
- Argus Notifier Plugin, 1.0.1 eta lehenagoko bertsioak.
- Artifactory Plugin, 2.16.1 eta lehenagoko bertsioak.
- Chatter Notifier Plugin, 2.0.4 eta lehenagoko bertsioak.
- Config File Provider Plugin, 3.1 eta lehenagoko bertsioak.
- Crowd 2 Integration Plugin, 2.0.0 eta lehenagoko bertsioak.
- Dimensions Plugin, 0.8.14 eta lehenagoko bertsioak.
- Email Extension Template Plugin, 1.0 eta lehenagoko bertsioak.
- Git Changelog Plugin, 2.6 eta lehenagoko bertsioak.
- HipChat Plugin, 2.2.0 eta lehenagoko bertsioak.
- JIRA Plugin, 3.0.1 eta lehenagoko bertsioak.
- Job Configuration History Plugin, 2.18 eta lehenagoko bertsioak.
- JUnit Plugin, 1.25 eta lehenagoko bertsioak.
- mesos Plugin, 0.17.1 eta lehenagoko bertsioak.
- Metadata Plugin, 1.1.0b eta lehenagoko bertsioak.
- Monitoring Plugin, 1.73.1 eta lehenagoko bertsioak.
- MQ Notifier Plugin, 1.2.6 eta lehenagoko bertsioak.
- PAM Authentication Plugin, 1.3 eta lehenagoko bertsioak.
- Publish Over Dropbox Plugin, 1.2.4 eta lehenagoko bertsioak.
- Rebuilder Plugin, 1.28 eta lehenagoko bertsioak.
- SonarQube Scanner Plugin, 2.8 eta lehenagoko bertsioak.

Azalpena:

Jenkins proiektuen automatizazio eta hedatze softwarean dauden hainbat ahultasunen berri eman da. Urruneko erasotzaile batek ahultasun horiek balia litzake hainbat eratako erasoak egiteko: gune gurutzatuetan eskaeraren faltsutzea (CSRF), kode gaiztoaren injekzioa (XSS) bai iraunkorra eta bai islatua, pribilegiorik gabeko erabiltzaileen aldetik kredentzialen zerrendatzea, eskarien faltsutzea zerbitzariaren aldean (SSRF), testu lauan gordetako kredentzialak eskuratzea edo kontuetara sartzea balioztatze egokirik gabe.

Konponbidea:

- Arachni Scanner Plugin 1.0.0 bertsiora eguneratu beharra dago.
- Argus Notifier Plugin 1.0.2 bertsiora eguneratu beharra dago.
- Artifactory Plugin 2.16.2 bertsiora eguneratu beharra dago.
- Chatter Notifier Plugin 2.0.5 bertsiora eguneratu beharra dago.
- Config File Provider Plugin 3.2 bertsiora eguneratu beharra dago.
- Crowd 2 Integration Plugin 2.0.1 bertsiora eguneratu beharra dago.
- Dimensions Plugin 0.8.15 bertsiora eguneratu beharra dago.
- Email Extension Template Plugin 1.1 bertsiora eguneratu beharra dago.
- Git Changelog Plugin 2.7 bertsiora eguneratu beharra dago.
- HipChat Plugin 2.2.1 bertsiora eguneratu beharra dago.
- JIRA Plugin 3.0.2 bertsiora eguneratu beharra dago.

- Job Configuration History Plugin 2.18.1 bertsiora eguneratu beharra dago.
- JUnit Plugin 1.26 bertsiora eguneratu beharra dago.
- mesos Plugin 0.18 bertsiora eguneratu beharra dago.
- Metadata Plugin-ek oraindik ez du eskuragarri *fix*-ik.
- Monitoring Plugin 1.74.0 bertsiora eguneratu beharra dago.
- MQ Notifier Plugin 1.2.7 bertsiora eguneratu beharra dago.
- PAM Authentication Plugin 1.4 bertsiora eguneratu beharra dago.
- Publish Over Dropbox Plugin 1.2.5 bertsiora eguneratu beharra dago.
- Rebuilder Plugin 1.29 bertsiora eguneratu beharra dago.
- SonarQube Scanner Plugin 2.8.1 bertsiora eguneratu beharra dago.

Xehetasuna:

Ahultasun guztien artetik, soilik ondokoa da kritikotasun altukoa:

- SECURITY-1156: Monitoring Plugin-eko JavaMelody liburutegiak XML External Entity-ren (XXE) prozesamendu erako ahultasun bat dauka. Hori baliatuz erasotzaile batek eskaera landuak bidal ditzake web aplikazio batera, fitxategien sistemaren informazioa eskuratzeko, zerbitzariaren aldean eskaerak faltsutzeko (SSRF) edo zerbitzuaren ukapen erasoak egiteko (DoS). Ahultasun horretarako CVE-2018-15531 identifikatzailea erreserbatu da.

Kritikotasun ertain eta baxuko beste ahultasun batzuk ere argitaratu dira, honako identifikatzaile hauekin: SECURITY-130, SECURITY-265, SECURITY-813 (CVE-2017-12197), SECURITY-845, SECURITY-938, SECURITY-948, SECURITY-972, SECURITY-984 (2), SECURITY-1011 (2), SECURITY-1013 (2), SECURITY-1029, SECURITY-1050 (2), SECURITY-1065, SECURITY-1067, SECURITY-1068, SECURITY-1075, SECURITY-1080, SECURITY-1101, SECURITY-1108, SECURITY-1122, SECURITY-1125, SECURITY-1130, SECURITY-1135, eta SECURITY-1163.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun HPE produktuetan

Argitalpen data: 2018/09/27

Garrantzia: Handia

Kaltetutako baliabideak:

- HPE SGF 4.2, RHEL 6 eta RHEL 7rako
  - E-Media SGF 4.2
  - Media SGF 4.2
- HPE SGF 4.3, RHEL 6 eta RHEL 7rako
  - E-Media SGF 4.3
  - Media SGF 4.3
- HPE Intelligent Management Center (iMC), iMC PLAT 7.3 E0605P04 baino lehenagokoa

Azalpena:

Hainbat ahultasun aurkitu dira HPEren hainbat produktutan:

- HPE Service Governance Framework-en (SGF) informazioaren urruneko zabalkunde baimen gabea gerta liteke.
- HPE Intelligent Management Center (iMC) PLATen kodearen urruneko exekuzioa gerta liteke.

Konponbidea:

- HPE Service Governance Framework-ek (SGF) duen informazioaren urruneko zabalkunde baimen gabearen ahultasunaren kasuan, SGF eguneratu beharra dago HPEren laguntza eskatuz, eskuragarri dagoen segurtasun partxea eman dezan.
- HPE Intelligent Management Center (iMC) PLATek duen kodearen urruneko exekuzioaren ahultasunaren kasuan, iMC PLAT 7.3 E0605P04 bertsioan konponduta dago, eta eguneraketa horretan jasotzen diren HPren sare produktuen zerrenda webgunearen *Resolution* atalean ageri da.

Xehetasuna:

Asmo gaiztoko erabiltzaile batek aipatutako ahultasunak baliatuko balitu, kaltetutako produktuetan ondoko ekintzak egin litzake:

- HPE Service Governance Framework-en (HPE SGF) karga altuko lasterketa egoera gerta liteke, SGFk parametro ezberdinak transferitzen dizkionean gaitzaileari. Horrek informazioaren urruneko zabalkunde baimengabe erako ahultasuna sortzen du. Ahultasun horretarako CVE-2018-7110 identifikatzailea erreserbatu da.
- HPE Intelligent Management Center (iMC) PLATek duen segurtasun ahultasun bat kodea urrunetik exekutatzeko balia liteke. Ahultasun honetarako CVE-2018-7076, CVE-2017-17485, CVE-2017-7525, CVE-2017-9096, CVE-2018-5968 eta CVE-2018-7489 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, HP, Ahultasuna

Ahultasuna TP-Link-en EAP softwarean

Argitalpen data: 2018/09/27

Garrantzia: Handia

Kaltetutako baliabideak:

- EAP Controller, 2.5.3 eta lehenagoko bertsioak.

Azalpena:

TP-Link EAP kontrolatzaileak ez dauka RMI autentifikaziorik eta deserializazio erasoek kaltetu egin dezakete.

Konponbidea:

Une honetan EAP kontrolatzailearentzat ez dago ahultasuna osorik konpontzen duen eguneraketarik eskuragarri. Nolanahi ere, TP-Linkek

gomendatzen du hainbat neurri hartzea arriskua arintzen eta murrizten laguntzeko.

- Apache Commons Collections eguneratzea
- EAPren JRE azken bertsiora eguneratzea

Xehetasuna:

Linuxerako TP-Link EAP sotwareak, haririk gabeko sarbide puntuko (WAP) gailuak urrunetik kontrolatzea ahalbidetzen duena, ez dauka erabiltzaile autentifikaziorik RMI zerbitzuko komandoetarako. Gainera, Apache Commons Collections-en bertsio zaharkitu eta ahul bat erabiltzen du. Urruneko erasotzaile batek deserializazio erasoak egin litzake RMI protokoloaren bidez, EAP Controller zerbitzaria urrunetik kontrola lezake eta Java edo bytecode Java funtzioak exekuta litzake. Apache Commons Collections ahultasunerako CVE-2015-6420 identifikatzailea erabili da. Eta EAP kontrolatzailearen ahultasunerako CVE-2018-5393 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Apache, Komunikazioak, Java, Ahultasuna

---

Hainbat ahultasun Netgear-en produktuetan

Argitalpen data: 2018/09/27

Garrantzia: Handia

Kaltetutako baliabideak:

- D3600, firmwarearen 1.0.0.76 bertsioa baino lehenagokoak
- D6000, firmwarearen 1.0.0.76 bertsioa baino lehenagokoak
- R6700, firmwarearen 1.0.1.48 bertsioa baino lehenagokoak
- R7500, firmwarearen 1.0.0.124 bertsioa baino lehenagokoak
- R7800, firmwarearen 1.0.2.58 bertsioa baino lehenagokoak
- R8900, firmwarearen 1.0.4.2 bertsioa baino lehenagokoak
- R9000, firmwarearen 1.0.4.2 bertsioa baino lehenagokoak
- WNDR3700v4, firmwarearen 1.0.2.102 bertsioa baino lehenagokoak
- WNDR4300v1, firmwarearen 1.0.2.104 bertsioa baino lehenagokoak
- WNDR4300v2, firmwarearen 1.0.0.56 bertsioa baino lehenagokoak
- WNDR4500v3, firmwarearen 1.0.0.56 bertsioa baino lehenagokoak
- WNR2000v5 (R2000), firmwarearen 1.0.0.68 bertsioa baino lehenagokoak
- R7900, firmwarearen 1.0.2.16 bertsioa baino lehenagokoak
- R6900, firmwarearen 1.0.1.48 bertsioa baino lehenagokoak
- R7000P, firmwarearen 1.3.1.44 bertsioa baino lehenagokoak
- R6900P, firmwarearen 1.3.1.44 bertsioa baino lehenagokoak
- R6250, firmwarearen 1.0.4.30 bertsioa baino lehenagokoak
- R6300v2, firmwarearen 1.0.4.32 bertsioa baino lehenagokoak
- R6400, firmwarearen a1.0.1.44 bertsioa baino lehenagokoak
- R6400v2, firmwarearen 1.0.2.60 bertsioa baino lehenagokoak
- R7000, firmwarearen 1.0.9.34 bertsioa baino lehenagokoak
- R7100LG, firmwarearen 1.0.0.48 bertsioa baino lehenagokoak
- R7300, firmwarearen 1.0.0.68 bertsioa baino lehenagokoak
- R8000, firmwarearen 1.0.4.18 bertsioa baino lehenagokoak
- R8000P, firmwarearen 1.4.1.24 bertsioa baino lehenagokoak
- R7900P, firmwarearen 1.4.1.24 bertsioa baino lehenagokoak
- R8500, firmwarearen 1.0.2.122 bertsioa baino lehenagokoak
- R8300, firmwarearen 1.0.2.122 bertsioa baino lehenagokoak
- WN2500RPv2, firmwarearen 1.0.1.54 bertsioa baino lehenagokoak
- EX3700, firmwarearen 1.0.0.72 bertsioa baino lehenagokoak
- EX3800, firmwarearen 1.0.0.72 bertsioa baino lehenagokoak
- EX6000, firmwarearen 1.0.0.32 bertsioa baino lehenagokoak
- EX6100, firmwarearen 1.0.2.24 bertsioa baino lehenagokoak
- EX6120, firmwarearen 1.0.0.42 bertsioa baino lehenagokoak
- EX6130, firmwarearen 1.0.0.24 bertsioa baino lehenagokoak
- EX6150v1, firmwarearen 1.0.0.42 bertsioa baino lehenagokoak
- EX6200, firmwarearen 1.0.3.88 bertsioa baino lehenagokoak
- EX7000, firmwarearen 1.0.0.66 bertsioa baino lehenagokoak
- D7000v2, firmwarearen 1.0.0.51 bertsioa baino lehenagokoak
- D6220, firmwarearen 1.0.0.46 bertsioa baino lehenagokoak
- D6400, firmwarearen 1.0.0.82 bertsioa baino lehenagokoak
- D8500, firmwarearen 1.0.3.42 bertsioa baino lehenagokoak
- WAC505, firmwarearen 5.0.0.17 bertsioa baino lehenagokoak
- WAC510, firmwarearen 5.0.0.17 bertsioa baino lehenagokoak
- WAC720, firmwarearen 5.0.0.17 bertsioa baino lehenagokoak
- WAC730, firmwarearen 5.0.0.17 bertsioa baino lehenagokoak
- WAC740, firmwarearen 5.0.0.17 bertsioa baino lehenagokoak
- WND930, firmwarearen 5.0.0.17 bertsioa baino lehenagokoak
- WC7500, firmwarearen 6.5.3.9 bertsioa baino lehenagokoak
- WC7520, firmwarearen 6.5.3.9 bertsioa baino lehenagokoak
- WC7600v1, firmwarearen 6.5.3.9 bertsioa baino lehenagokoak
- WC7600v2, firmwarearen 6.5.3.9 bertsioa baino lehenagokoak
- GS110EMX, firmwarearen 1.0.0.9 bertsioa baino lehenagokoak
- GS810EMX, firmwarearen 1.0.0.5 bertsioa baino lehenagokoak
- XS512EM, firmwarearen 1.0.0.6 bertsioa baino lehenagokoak
- XS724EM, firmwarearen 1.0.0.6 bertsioa baino lehenagokoak
- WAC505, firmwarearen 5.0.5.4 bertsioa baino lehenagokoak
- WAC510, firmwarearen 5.0.5.4 bertsioa baino lehenagokoak
- XR500, firmwarearen 2.3.2.32 bertsioa baino lehenagokoak

Azalpena:

Ohartarazpen honek Netgear produktuei eragiten dieten 24 ahultasun jasotzen ditu eta horietatik 18 larritasun altukoak dira.

Konponbidea:

Firmwarearen azken bertsiora eguneratzea, webgunean eskuragarri: https://www.netgear.com/support/.

Xehetasuna:

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

- Autentifikazioari ihes egitea
- Informazio sentikorrera sarbidea izatea
- Autentifikazioaren ondoren pilari (stack) gainezka eginaraztea
- Autentifikazioa baino lehen pilari (stack) gainezka eginaraztea
- Firmwarearen aurreko bertsio bat instalatzea
- Autentifikazioa baino lehen komandoak injektatzea
- Autentifikazioaren ondoren komandoak injektatzea
- Pribilegioen eskalatze bertikala
- Zerbitzua ukatzea
- Cross-site request forgery
- Segurtasunaren konfigurazio oker bat egitea

Etiketak: Eguneraketa, Pribatutasuna, Ahultasuna

Ahultasuna TP-Link-en EAP softwarean

Argitalpen data: 2018/09/27

Garrantzia: Handia

Kaltetutako baliabideak:

- EAP Controller, 2.5.3 eta lehenagoko bertsioak.

Azalpena:

TP-Link EAP kontrolatzaileak ez dauka RMI autentifikaziorik eta deserializazio erasoek kaltetu egin dezakete.

Konponbidea:

Une honetan EAP kontrolatzailearentzat ez dago ahultasuna osorik konpontzen duen eguneraketarik eskuragarri. Nolanahi ere, TP-Linkek gomendatzen du hainbat neurri hartzea arriskua arintzen eta murrizten laguntzeko.

- Apache Commons Collections eguneratzea
- EAPren JRE azken bertsiora eguneratzea

Xehetasuna:

Linuxerako TP-Link EAP sotwareak, haririk gabeko sarbide puntuko (WAP) gailuak urrunetik kontrolatzea ahalbidetzen duena, ez dauka erabiltzaile autentifikaziorik RMI zerbitzuko komandoetarako. Gainera, Apache Commons Collections-en bertsio zaharkitu eta ahul bat erabiltzen du. Urruneko erasotzaile batek deserializazio erasoak egin litzake RMI protokoloaren bidez, EAP Controller zerbitzaria urrunetik kontrola lezake eta Java edo bytecode Java funtzioak exekuta litzake. Apache Commons Collections ahultasunerako CVE-2015-6420 identifikatzailea erabili da. Eta EAP kontrolatzailearen ahultasunerako CVE-2018-5393 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Apache, Komunikazioak, Java, Ahultasuna

---

Birbideratze ireki motako ahultasuna IBMren WebSphere Portal-en

Argitalpen data: 2018/09/27

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM WebSphere Portal, 9.0.0.0tik 9.0.0.0 CF15era bitarteko bertsioak
- IBM WebSphere Portal, 8.5.0.0tik 8.5.0.0 CF15era bitarteko bertsioak
- IBM WebSphere Portal, 8.0.0.0tik 8.0.0.1 CF23ra bitarteko bertsioak
- IBM WebSphere Portal, 7.0.0.0tik 7.0.0.2 CF30era bitarteko bertsioak

Azalpena:

IBM WebSphere Portalek urruneko erasotzaile bati phishing erasoak egitea ahalbidetu liezaioke, birbideratze irekiko eraso bat erabiliz.

Konponbidea:

- 8.5 eta 9.0 bertsioen kasuan, CF16ra eguneratu
- 8.0.0.0tik 8.0.0.1era bitarteko bertsioen kasuan, Fix Pack 8.0.0.1 CF 23ra eguneratu eta ondoren Interim Fix PH01459 aplikatu
- 7.0.0.0tik 7.0.0.2ra bitarteko bertsioen kasuan, Fix Pack 7.0.0.2 CF 30era eguneratu eta ondoren Interim Fix PH01459 aplikatu

Xehetasuna:

- Biktima bat konbentzitu ondoren bereziki diseinatutako webgune bat bisita dezan, urruneko erasotzaile batek ahultasun hau balia lezake erakutsitako URLa faltsutzeko eta erabiltzaile bat webgune gaizto batera birbideratzeko. Horri esker erasotzaileak informazio oso sentikorra eskura lezake edo biktimaren aurkako eraso berriak egin. Ahultasun horretarako CVE-2018-1736 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Cisco IOS eta IOS XE-n

Argitalpen data: 2018/09/27

Garrantzia: Handia

Kaltetutako baliabideak:

- Cisco IOS eta IOS XE Softwareren bertsio ahulak exekutatzen dituzten gailuak, OSPFv3 eragiketak egiteko konfiguratuak.
- Cisco IOS XE softwarea honako hauetan:
  - Cisco ASR 1000 Series Aggregation Services Routers:
    - ASR 1001-X
    - ASR 1001-HX
    - ASR 1002-X
    - ASR 1002-HX
    - Cisco ASR 1000 Series 100-Gbps Embedded Service Processor (ASR1000-ESP100)
    - Cisco ASR 1000 Series 200-Gbps Embedded Service Processor (ASR1000-ESP200)
  - Cisco 4000 Series Integrated Services Routers:
    - ISR 4431
    - ISR 4451-X
  - Softwarea IPsec VPN konexioak amaitzeko konfiguratuta badago, ondokoa barne:
    - LAN-to-LAN VPN
    - Remote-access VPN, excluding SSL VPN
    - Dynamic Multipoint VPN (DMVPN)
    - FlexVPN
    - Group Encrypted Transport VPN (GET VPN)
    - IPsec virtual tunnel interfaces (VTIs)
    - Open Shortest Path First Version 3 (OSPFv3), IPSec-ekin autentifikatzeko zerbitzuarekin
- Cisco ASA softwarea eta Cisco ASA 5500-X seriea Firepower Threat Defense softwarearekin
  - ASA 5506-X seriea
  - ASA 5508-X seriea
  - ASA 5516-X seriea
- Swiches Cisco Catalyst 3650 eta 3850 serieak, 16.1.1 bertsioa
- Cisco IOS XE Software, HTTP zerbitzari ezaugarria gaituta.
- Cisco ISR G2 edo Cisco ISR4451-X Routers, SM-X-1T3/E3 modulu bat instalatuta badute eta Cisco IOS edo IOS XE Softwareren bertsio kaltetu bat exekutatzen ari badira.
- Cisco IOS XE Software, NATerako konfiguratuta eta gailuan NAT konfiguratzen denean SIP ALG aktibatzen bada.
- Cisco IOS Software edo Cisco IOS XE Softwareren bertsio kaltetu bat exekutatzen duten Cisco Catalyst Switches, kluster funtzioa gaituta dutela eta klusterreko kide ez baziren azken birkargaz geroztik.
- Cisco IOS XE Softwarea exekutatzen duten gailuak, 16.6.1 edo 16.6.2 bertsioak, eta CDP funtzioa aktibatuta dutenak gutxienez interfaze batean.
- Cisco Catalyst 3650, 3850 eta 4500E, Cisco IOS XEren bertsio kaltetu bat exekutatzen dutenak eta errdisable funtzioa gaituta dutenak funtzio baterako, bai VLAN eta bai ataka mailan.
- Cisco IOS XE Software.
- Cisco IOS Software edo Cisco IOS XE Software, IPv6rekin konfiguratuta.
- Cisco IOS Software, PTP (Precision Time Protocol) paketeak prozesatzeko konfiguratuta:
  - 2500 Series Connected Grid Switches
  - Connected Grid Ethernet Switch Module Interface Card
  - Industrial Ethernet 2000 Series Switches
  - Industrial Ethernet 2000U Series Switches
  - Industrial Ethernet 3000 Series Switches
  - Industrial Ethernet 3010 Series Switches
  - Industrial Ethernet 4000 Series Switches
  - Industrial Ethernet 4010 Series Switches
  - Industrial Ethernet 5000 Series Switches

Azalpena:

Ciscok 12 segurtasun ohartarazpen argitaratu ditu Cisco IOSen 13 ahultasun azaltzen dituztenak, guztiak kritikotasun altukoak.

Konponbidea:

Ciscok kaltetutako produktuen bertsio berrienetara eguneratzea aholkatzen du. Ondoko loturan eskura daitezke:

· Software Ciscoren deskarga panela

Xehetasuna:

Ondoren zehazten dira 13 ahultasunak:

- Open Shortest Path First-en inplementazioan 3. bertsioak (OSPFv3) Cisco IOS eta IOS XE Software-n duen ahultasun bat baliatuz, gertuan dagoen eta autentifikatuta dagoen erasotzaile batek kaltetutako gailua birkargatzea eragin lezake, zerbitzuaren ukapen egoera sortuz (DoS). Ahultasun hau OSPFv3 pakete espezifikoen erabilera oker batek sortua da. Ahultasun horretarako CVE-2018-0466 identifikatzailea erreserbatu da.
- Cisco IOS XE softwarearen hainbat plataformaren eta Cisco ASA 5500-X serieko segurtasun gailu egokigarriaren (ASA) IPSec kontrolatzailearen kodeak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek gailua birkargatzea eragin lezake. Ahultasunaren arrazoia da gaizki osatutako IPSec autentifikazioaren goiburuaren (AH) prozesamendu oker bat edo Encapsulating Security Payload (ESP). Ahultasun horretarako CVE-2018-0472 identifikatzailea erreserbatu da.
- Cisco IOS XE softwareak web erabiltzailearen interfazean duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek kaltetutako gailua birkargatzea eragin lezake, zerbitzuaren ukapen egoera sortuz (DoS). Ahultasun honen arrazoia kaltetutako softwareak duen double-free-in-memory akats bat da, HTTP eskari espezifikoak prozesatzen direnean. Ahultasun horretarako CVE-2018-0469 identifikatzailea erreserbatu da.
- Cisco IOS XE softwareak web markoan duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek bufferraren gainezkatzea eragin lezake kaltetutako gailu batean, eta horrek zerbitzuaren ukapen egoera (DoS) sor lezake. Ahultasunaren arrazoia da kaltetutako softwareak modu okerrean aztertzen dituela gailu bati zuzendutako HTTP pakete gaizki osatuak. Ahultasun horretarako CVE-2018-0470 identifikatzailea erreserbatu da.
- Ciscoren bigarren belaunaldiko zerbitzu integratuen (ISR G2) SM-1T3/E3 routerren eta zerbitzu integratuen Cisco 4451-X (ISR4451-X) routerraren firmwareak duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek lor lezake ISR G2 routerra edo ISR4451-X gailuaren SM-1T3/E3 modulua birkargatzea, eta horrek zerbitzuaren ukapen egoera (DoS) sor lezake. Ahultasunaren arrazoia da erabiltzailearen sarreraren maneiu desegoki bat. Ahultasun horretarako CVE-2018-0485 identifikatzailea erreserbatu da.
- Cisco IOS XE softwareak Network Address Translation (NAT) Session Initiation Protocol (SIP) Application Layer Gateway-en (ALG) duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek kaltetutako gailu baten birkarga eragin lezake. Ahultasun horretarako CVE-2018-0476 identifikatzailea erreserbatu da.
- Cisco IOS Software eta Cisco IOS XE Software-ren klusterrak duen sarbidearen balioztatze okerreko ahultasun bat baliatuz, autentifikaziorik gabeko erasotzaile batek switcha blokeatzea edo gainkargatzea lor lezake, ICMP mezu gaizto bat bidaliz. Ahultasun horretarako CVE-2018-0475 identifikatzailea erreserbatu da.
- CDP pakete jakin batzuen prozesatze oker bat baliatuz, autentifikaziorik gabeko erasotzaile batek zerbitzuaren ukapen egoera sortuko lukeen memoriaren ihesa eragin lezake. Ahultasun horretarako CVE-2018-0471 identifikatzailea erreserbatu da.

- VLAN eta ataka bat errsdisabled egoeran sartzen direnean gertatzen den lasterketa baldintza bat baliatuz, erasotzaile batek switcha blokeatzea edo gainkargatzea lor lezake, zerbitzuaren ukapen egoera eraginez. Ahultasun horretarako CVE-2018-0480 identifikatzailea erreserbatu da.
- Cisco IOS XE Software-ren CLI analizatzaileak dituen hainbat ahultasun baliatuz, autentifikatuta dagoen erasotzaile lokal batek komandoak exekuta litzake kaltetutako gailu baten azpiko Linux shell-ean, administratzaile pribilegioekin. Ahultasun horietarako CVE-2018-0477 eta CVE-2018-0481 identifikatzaileak erreserbatu dira.
- Cisco IOS Software eta CiscoIOS XE Software-ren IPv6ren prozesamendu kodeak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek gailua berrabiaraztea eragin lezake. Ahultasun horretarako CVE-2018-0467 identifikatzailea erreserbatu da.
- Cisco IOS softwarearen Precision Time Protocol (PTP) azpisistemak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek PTPan zerbitzuaren ukapen egoera (DoS) sor lezake. Ahultasun horretarako CVE-2018-0473 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Komunikazioak, Ahultasuna

XML Entity Expansion erako ahultasuna IBM Platform Symphony-n eta IBM Spectrum Symphony-n

Argitalpen data: 2018/09/28

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM Platform Symphony 7.1 Fix Pack 1 eta 7.1.1
- IBM Spectrum Symphony 7.1.2 eta 7.2.0.2

Azalpena:

XML Entity Expansion (XXE) erako ahultasunak IBM Platform Symphony eta IBM Spectrum Symphony produktuei eragiten die.

Konponbidea:

Segurtasun partxeak IBM Fix Central-etik jaits daitezke:

- sym-7.1-build494537
- sym-7.1.1-build494444
- sym-7.1.2-build494315
- sym-7.2.0.2-build494326

Xehetasuna:

IBM Spectrum Symphony-k XML External Entity Injection (XXE) erako eraso bat jasan lezake XML datuak prozesatzean. Urruneko erasotzaile batek ahultasun hori balia lezake informazio konfidentziala agerian uzteko edo memoriaren baliabideak kontsumitzeko. Ahultasun horretarako CVE-2018-1702 identifikatzailea erreserbatu da.

Etiketak: IBM, Ahultasuna