2018ko Abenduaren Bulletina

Ohartarazpenak - Teknikoak

Ahultasuna Mbed-en TLSn

Argitalpen data: 2018/12/04

Garrantzia: Handia

Kaltetutako baliabideak:

- Mbed TLSren bertsio guztiak.

Azalpena:

Kritikotasun altuko ahultasuna baliatuz, pribilegiorik gabeko erasotzaile lokal batek RSA-sin-(EC)DH(E) zifratuko suiteetan erabiltzen den RSA deszifratuaren testu laua eskura lezake.

Konponbidea:

- Mbed TLSren bertsio berrienetakoren batera eguneratzea, 2.14.1, 2.7.8, 2.1.17 edo berriagoak barne.
- Mbed TLSren bertsio eguneratuak oraindik ahulak dira ihesetako baten aurrean, baldin eta RSA gakoaren tamaina ez bada makinaren hitzaren tamainaren multiploa. Horregatik aholkatzen da 64 biten multiploak diren gako tamainak erabiltzea.

Xehetasuna:

- Ahultasuna baliatuz erasotzaile batek kodea exekuta lezake eta formaturik gabeko testua berreskuratu *Bleichenbacher oracle* baten bidez. Zehazki, RSA deszifratua erabiltzen duten (D)TLS konexioei eragiten die. Horietan erasotzaileak konexioa deszifra lezake zerbitzarian testua berreskuratzeko eraso baten bidez, edo konexioa atzeman dezake edukiaren gaineko man-in-the-middle erako eraso baten bidez. Ahultasun horretarako CVE-2018-19608 kodea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun IBMren produktuetan

Argitalpen data: 2018/12/05

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM Campaign, 9.1.0 eta 9.1.2 bertsioak
- IBM QRadar SIEM, 7.2.0tik 7.2.8 Patch 13ra bitarteko bertsioak eta 7.3.0tik 7.3.1 Patch 6ra bitartekoak

Azalpena:

IBMk bere Campaign eta QRadar SIEM produktuek dituzten hainbat ahultasunen berri eman du. Horiek baliatuz pribilegioen eskalatzea, informazioaren zabalkundea edo zerbitzuaren ukapena eragin litezke.

Konponbidea:

- IBM Campaign-en 9.1.0ren kasuan, 9.1.0.13 bertsiora eguneratu
- IBM Campaign-en 9.1.2ren kasuan, 9.1.2.7 bertsiora eguneratu
- IBM QRadar SIEMen kasuan, 7.2.0tik 7.2.8 Patch 13ra bitarteko bertsioetan, QRadar / QRM / QVM / QRIF / QNI 7.2.8 Patch 14 bertsiora eguneratu
- IBM QRadar SIEMen kasuan, 7.3.0tik 7.3.1 Patch 6ra bitarteko bertsioetan, QRadar / QRM / QVM / QRIF / QNI 7.3.1 Patch 7 bertsiora eguneratu

Xehetasuna:

- IBM Campaign baliatuz erabiltzaile lokal batek administratzaile pribilegioak eskura litzake aplikazioak sarbide baimenak ez dituelako baliozkotzen. Ahultasun horretarako CVE-2018-1941 identifikatzailea erreserbatu da.

- IBM QRadar-ek XML *External Entity Injection* (XXE) erako eraso bat jasan lezake XML datuak prozesatzean. Hori baliatuz urruneko erasotzaile batek informazio sentikorra agerian utz lezake edo memoriako baliabideak kontsumitu. Ahultasun horretarako CVE-2018-1730 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Jenkins-en

Argitalpen data: 2018/12/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Jenkins Weekly, 2.153 eta lehenagoko bertsioak.
- Jenkins LTS, 2.138.3 eta lehenagoko bertsioak.

Azalpena:

Jenkinsek hainbat produkturi buruzko 4 ahultasun argitaratu ditu, horietatik 1 larritasun kritikokoa eta 3 larritasun ertainekoak.

Konponbidea:

- Jenkins Weekly eguneratu 2.154 bertsiora
- Jenkins LTS eguneratu 2.138.4 edo 2.150.1 bertsioetara

Xehetasuna:

Ondoren larritasun kritikoko ahultasuna soilik zehazten da, SECURITY-595 identifikatzailea duena.

- HTTP eskaerak maneiatzeko, Jenkins-ek *Stapler* web framework-a erabiltzen du eta honek bere nomenklaturaren konbentzioekin bat datozen kode elementuetarako sarbide erreflexiboa erabiltzen du. Horiek oso estuki bat datozenez Javan ohikoak diren kode patroiekin, diseinatutako URLetarako sarbideak metodo batzuk dei litzake inoiz modu horretara deitu nahiko ez zirenak. Horren ondorioz:
  - Autentifikaziorik gabeko erabiltzaileek saio guztiak baliogabetu litzakete Jenkins exekutatzen dutenean *Winstone-Jetty* zerbitzaria integraturik.
  - *Overall/Read* baimena duten erabiltzaileek memorian erabiltzailearen objektu berriak sor litzakete.
  - *Overall/Read* baimena duten erabiltzaileek *AsyncPeriodicWork* inplementazioen exekuzioak eskuz has litzakete, bestela aldizka exekutatuko liratekeenak.

Gainerako ahultasunetarako Jenkins-ek honako identifikatzaileak erabili ditu: SECURITY-904, SECURITY-1072 eta SECURITY-1193

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun IBMren Cloud Kubernetes Service eta Marketing Platform-en

Argitalpen data: 2018/12/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IBM Cloud Kubernetes Service, 1.12.0tik 1.12.2ra bitarteko bertsioak, 1.11.0tik 1.11.4ra bitartekoak, 1.10.0tik 1.10.10ra bitartekoak eta 1.5etik 1.9ra bitartekoak.
- IBM Marketing Platform, 9.1.0, 9.1.2 eta 10.1 bertsioak.

Azalpena:

IBMk hainbat ahultasunen berri eman du. Horiek baliatuz baimenik gabeko sarbidea edo pribilegioen eskalatzea lor liteke Kubernetes API Server-en eta informazioaren zabalkundea edo memoriaren kontsumoa IBM Marketing Platform-en.

Konponbidea:

- IBM Clud Kubernetes Service-ren kasuan, zure *clúster*-aren bertsioa begiratu *ibmcloud ks clusters* komandoaren bidez eta ondokoa egiaztatu:
  - 1.10 bertsioa eta geroagokoak eguneratuak izan dira erabiltzaileen esku hartzea behar izan gabe.
  - 1.12.3, 1.11.5 eta 1.10.11 bertsioei ahultasunak ez die eragiten.
  - *Clúster*-a 1.10, 1.11 edo 1.12 bertsioetan badago eta automatikoki ez bada eguneratu, IBM Cloud Support zerbitzuarekin harremanetan jarri laguntza lortzeko.
  - 1.8 eta 1.9 bertsioak 1.10, 1.11 edo 1.12 bertsioetara eguneratu behar dira.
  - 1.7 bertsioa lehenik 1.9 bertsiora eguneratu behar da, eta ondoren 1.10, 1.11 edo 1.12 bertsioetara.
  - 1.5 bertsioa ezin da eguneratu.
- IBM Marketing Platform-en kasuan:
  - 9.1.0 bertsioa 9.1.0.13 bertsiora eguneratu
  - 9.1.2 bertsioa 9.1.2.6-IBM_MP-IF01 bertsiora eguneratu
  - 10.1 bertsioa 10.1.0.1 bertsiora eguneratu

Xehetasuna:

- Kubernetes-en API zerbitzarian eskarien erabilpen desegoki bat baliatuz, urruneko erasotzaile batek, *backend*-era zuzenean bidal lezakeen bereziki diseinatutako proxy eskari baten bidez, konexioa ezar lezake, zerbitzu kudeatuak sortu eta kode gaiztoa inplementatu pribilegio altuekin. Larritasun kritikoko ahultasun horretarako CVE-2018-1002105 kodea erabili da.
- IBM Marketing Platform-ek XML *External Entity Injection* (XXE) erako eraso bat jasan lezake XML datuak prozesatzean. Urruneko erasotzaile batek informazio sentikorra agerian utz lezake edo memoriaren baliabideak kontsumitu. Larritasun altuko ahultasun horietarako CVE-2018-1920 eta CVE-2018-1424 kodeak erreserbatu dira.

Etiketak: Eguneraketa, IBM, Ahultasuna

Ahultasuna F5en hainbat produktutan

Argitalpen data: 2018/12/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- BIG-IP (APM), ondoko bertsioak:
  - 14.0.0
  - 13.0.0 - 13.1.1
  - 12.1.0 - 12.1.3
- BIG-IP APM Clients, 7.1.5etik 7.1.7ra bitarteko bertsioak, biak barne.
- BIG-IP Edge Client, 7101etik 7150era bitarteko bertsioak, biak barne.

Azalpena:

Ahultasun hori arrakastaz baliatuz gero pribilegiorik gabeko erabiltzaile lokal batek informazio sentikorra ikus lezake, datu jakin batzuk manipulatu edo bezero lokalaren *host*-ean supererabiltzaile pribilegioak eskuratu.

Konponbidea:

- Kaltetutako BIG-IP (APM) bertsioen kasuan oraingoz ez dago konponbiderik.
- BIG-IP APM Clients-en kasuan, 7.1.7.2 bertsiora eguneratu.
- Kaltetutako BIG-IP Edge Client bertsioen kasuan oraingoz ez dago konponbiderik.

Xehetasuna:

- F5 BIG-IP APMren bezeroaren *svpn* osagaia pribilegiodun prozesu baten modura exekutatzen da, eta hori baliatuz, pribilegiorik gabeko erabiltzaile batek *root* atributuak dituzten fitxategien jabetza eskura lezake bezero lokalaren *host*-ean lasterketa baldintzetan. Ahultasun horretarako CVE-2018-15332 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

SAPen 2018ko abenduko segurtasun eguneraketa

Argitalpen data: 2018/12/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa
- SAP Commerce (SAP Hybris Commerce), 6.2, 6.3, 6.4, 6.5, 6.6, 6.7 bertsioak
- SAP Basis ("AS ABAP of SAP NetWeaver" 700etik 750era bitartekoak, 750etik aurrera "ABAP Platform" izenaz zabaldua) 7.00tik 7.02ra, 7.10etik 7.30era, 7.31, 7.40 eta 7.50etik 7.53ra bitarteko bertsioak
- SAP NetWeaver, ServerCore bertsioak (7.11, 7.20, 7.30, 7.31, 7.40, 7.50)
- SAP NetWeaver (Application Server Java Library), 7.20, 7.30, 7.31 eta 7.50 bertsioak
- SAP NetWeaver AS Java, ServerCore bertsioak (7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50)
- SAP ABAP Change and Transport System (CTS), SAP KERNEL 32 NUC, SAP KERNEL 32 Unicode, SAP KERNEL 64 NUC, SAP KERNEL 64 Unicode 7.21, 7.21EXT, 7.22 eta 7.22EXT bertsioak; SAP KERNEL 7.21, 7.22, 7.45, 7.49, 7.53, 7.73 eta 7.74 bertsioak
- SAP Marketing, UICUAN bertsioak (1.20, 1.30, 1.40), SAPSCORE (1.13, 1.14)
- SAP_BASIS, 6.40, 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 bertsioak
- SAP Business One Service Layer, B1_ON_HANA bertsioa (9.2, 9.3)
- SAP Mobile Secure for Android, 6.60.19942.0 SP28 1711 bertsioa
- SAP HANA, 1.0 eta 2.0 bertsioak

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 9 segurtasun ohar eta 3 eguneraketa eman ditu ezagutzera. Horietatik 2 larritasun kritikokoak dira, 3 larritasun altukoak, 6 larritasun ertainekoak eta 1 larritasun baxukoa.

Argitaratutako ahultasun motak ondokoak dira:

- Baimenaren egiaztapen gabeziako 2 ahultasun.
- Cross-site scripting erako 3 ahultasun.
- Informazio zabalkundeko ahultasun bat.
- XMLren balioztatze okerreko ahultasun bat.
- Cross-frame scripting erako ahultasun bat.
- Beste era batzuetako 4 ahultasun.

Larritasun kritikoak honakoak dira:

- SAP Business Client-en 6.5 bertsioak duen ahultasun bat baliatuz, erasotzaile bateko kode arbitrarioa exekuta lezake *sandbox* baten barnean aurrez diseinatutakoHTML orrialde baten bidez.
- SAP Hybris Commerce-k duen cross-site scripting (XSS) erako ahultasun batek *JavaScript webApplicationInjector.js* fitxategiari eragiten dio, edo horren kopia bati dendek erabiltzen dutenean.

Etiketak: Eguneraketa, SAP, Ahultasuna

2018ko abenduko Microsoften segurtasun buletina

Argitalpen data: 2018/12/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Adobe Flash Player.
- Internet Explorer.
- Microsoft Edge.
- Microsoft Windows.
- Microsoft Office eta Microsoft Office Services eta Web Apps.
- ChakraCore.
- . NET Framework.
- Microsoft Dynamics NAV.
- Microsoft Exchange Server.
- Microsoft Visual Studio.
- Windows Azure Pack (WAP).

Azalpena:

Segurtasun eguneraketei buruzko Microsoften hileroko argitalpenean 39 ahultasun jaso dira oraingoan, 9 kritiko gisa sailkatu dira eta 30 garrantzitsu gisa. Gainerakoak larritasun ertain edo baxukoak dira.

Konponbidea:

Dagozkien segurtasun eguneraketak instalatzea. Eguneraketen beraien instalazioaren informazio orrialdean hori egiteko metodo ezberdinei buruzko argibideak daude.

Xehetasuna:

Argitaratutako ahultasun motak ondokoak dira:

- Informazioa ezagutaraztea.
- Zerbitzuaren ukapena.
- Kodearen urruneko exekuzioa.
- Pribilegioen eskalatzea.
- Ordeztea (*spoofing*).
- Manipulatzea (*tampering*).

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

Hainbat ahultasun Intel-en produktuetan

Argitalpen data: 2018/12/12

Garrantzia: Handia

Kaltetutako baliabideak:

- Intel® Solid State Drive Toolbox, 3.5.7 baino lehenagoko bertsioak.
- Intel(R) VTune Amplifier 2018 Update 3 eta lehenagokoak.
- Intel® Parallel Studio, Intel® System Studio 2019 Gold baino lehenagokoa.
- Intel® System Defense Utility, bertsio guztiak.
- Linuxerako Intel(R) QuickAssist Technology.

Azalpena:

Intelek 5 segurtasun ohartarazpen argitaratu ditu larritasunei buruzko bere produktuen segurtasun zentroan: 1 altua, 3 ertainak eta 1 baxua.

Konponbidea:

- Intel® Solid State Drive Toolbox-en kasuan:
  - Aurretik dagoen Intel® Solid State Drive Toolbox-en bertsioa desinstalatu.
  - 3.5.7 edo berriagoa den bertsio batera eguneratu.
- Intel(R) VTune Amplifier-en kasuan:
  - Intel® VTune Amplifier 2019 Update 1 edo berriago batera eguneratu.
- Intel® Parallel Studio-ren kasuan:
  - v2019 Update 1 edo berriago batera eguneratu.
- Intel® System Defense Utility-ren kasuan:
  - Intelek utilitate honetarako produktuen etenaldi bat iragarriz ohartarazpen bat argitaratu du eta erabiltzaileei gomendatzen die lehenbailehen desinstalatzea edo erabiltzeari uztea.
- Intel(R) QuickAssist Technology-ren kasuan:
  - CVE-2018-12206: bertsioaren oharrak ebaluatu, 3.1.4 atala, VMren inplementazio ingurunean aldaketak egon diren antzemateko.
  - CVE-2018-18096: funtzionaltasuna ezabatu egin da R4.3n eta berriz ezarriko da R4.4 eta ondorengo bertsioetan.

Xehetasuna:

- 3.4.7 bertsioa baino lehenagoko Intel® Solid State Drive Toolbox-en baimen okerrak baliatuz, autentifikatutako erasotzaile batek pribilegioen eskalatzea gaitu lezake sarbide lokalaren bidez. Larritasun altuko ahultasun horretarako CVE-2018-18097 identifikatzailea erreserbatu da.

Larritasun ertain eta baxuko gainerako ahultasunetarako erreserbatu diren identifikatzaileak honakoak dira: CVE-2018-18093, CVE-2018-3704, CVE-2018-3705 eta CVE-2018-18096.

Etiketak: Eguneraketa, Ahultasuna

Kodearen urruneko exekuzioa IBMren WebSphere Application Server-en

Argitalpen data: 2018/12/12

Garrantzia: Handia

Kaltetutako baliabideak:

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

Azalpena:

IBMk larritasun altuko ahultasun bat argitaratu du bere WebSphere Application Server produktuari eragiten diona eta urrunetik kodea exekutatzea ahalbidetu lezakeena.

Konponbidea:

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* PH04060 ezartzea.
  - *Fixpack* 9.0.0.10 edo ondorengoa aplikatzea (2018ko laugarren 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* PH04060 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:
  - 8.0.0.15 bertsiora eguneratzea eta ondoren *Interim Fix* PH04060 aplikatzea.
- 7.0.0.0tik 7.0.0.45era bitarteko bertsioetarako:
  - 7.0.0.45 bertsiora eguneratzea eta ondoren *Interim Fix* PH04060 aplikatzea.

Xehetasuna:

- IBM WebSphere Application Server-ek duen ahultasun bat baliatuz urruneko erasotzaile batek Java kode arbitrarioa exekuta lezake bezero administratiboko mota baten bidez, iturri ez fidagarrietako objektu serializatu batekin. Ahultasun horretarako CVE-2018-1904 identifikatzailea erabili da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun WordPress-en

Argitalpen data: 2018/12/13

Garrantzia: Handia

Kaltetutako baliabideak:

- WordPress, 5.0 eta lehenagoko bertsioak.

Azalpena:

WordPressek segurtasun eguneraketa bat argitaratu du hainbat ikertzailek aurkitutako 7 ahultasun zuzentzeko.

Konponbidea:

- WordPress 5.0.1 bertsiora eguneratzea, beren deskarga zentroan eskuragarri.

Xehetasuna:

WordPressek guztira 7 ahultasunen berri eman du, era hauetakoak:

- Metadatuen aldaketa, baimenik gabe fitxategiak ezabatzeko.
- Baimendu gabeko argitalpenen sorrera bereziki diseinatutako sarrerarekin.
- PHPn objektuen injekzioa metadatuak aldatuz.
- Iruzkinen edizioan *Cross-site scripting* pribilegio altuekin.
- *Cross-site scripting* bereziki diseinatutako URL sarreretan.
- Email helbideak agerian uztea, eta kasu arraroetan pasahitzak, modu lehenetsian sortutakoak.
- *Cross-site scripting* Apache-n ostatatutako *host*-etan.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun phpMyAdmin-en

Argitalpen data: 2018/12/13

Garrantzia: Handia

Kaltetutako baliabideak:

phpMyAdmin-en ondoko bertsioak izan dira kaltetuak:

- 4.0tik 4.8.3ra bitartekoak
- 4.7.0tik 4.7.6ra eta 4.8.0tik 4.8.3ra bitartekoak

Azalpena:

phpMyAdmin-eko ekipoak 4.8.4 bertsioa argitaratu du, segurtasun zuzenketa garrantzitsu batzuk dituena.

Konponbidea:

- phpMyAdmin-eko 4.8.4 edo goragoko bertsiora eguneratzea gomendatzen da.

Xehetasuna:

- 4.0tik 4.8.3ra bitarteko bertsioek fitxategi lokalen inklusio akats bat daukate (Local File Inclusion, LFI). Hori baliatuz urruneko erasotzaile batek zerbitzariko fitxategi lokalak irakur litzake. Ahultasun horretarako CVE-2018-19968 identifikatzailea erabili da. Gainera, bertsio horietan *Cross-site Scripting* (XSS) erako beste ahultasun bat ere aurkitu da. Hori baliatuz erasotzaile batek kode gaiztoa injekta dezake bereziki diseinatutako taula/datu baseko izen baten bidez. Ahultasun horretarako CVE-2018-19970 identifikatzailea erabili da.
- 4.7.0tik 4.7.6ra eta 4.8.0tik 4.8.3ra bitarteko bertsioetan akats bat aurkitu da. Hori baliatuz, erasotzaile batek asmo txarreko SQL eragiketak egin litzake *Cross-site Request Forgery* (CSRF) eraso baten bidez. Ahultasun horretarako CVE-2018-19969 identifikatzailea erabili da.

Etiketak: Eguneraketa, PHP, Ahultasuna

Ahultasuna IBMren Operational Decision Manager-en

Argitalpen data: 2018/12/13

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM Operational Decision Manager, 8.6, 8.7, 8.8 eta 8.9 bertsioak

Azalpena:

IBMk bere Operational Decision Manager produktuak duen ahultasun baten berri eman du. Hori baliatuz, urruneko erasotzaile batek informazio sentikorra agerian utz lezake edo memoriako baliabideak kontsumitu.

Konponbidea:

ODMren instalazioa eguneratzeko, aukeratu ondoko behin-behineko konponbidea, zure produktuaren bertsioaren arabera:

APAR RS03231 eta RS03192rako Interim fix, IBM Fix Centralen eskuragarri:

- IBM Operational Decision Manager v8.6:
  - 8.6.0.3-WS-ODM_DS-IF035
- IBM Operational Decision Manager v8.7:
  - 8.7.1.2-WS-ODM_DS-IF079
- IBM Operational Decision Manager v8.8:
  - 8.8.1.3-WS-ODM_DS-IF090
- IBM Operational Decision Manager v8.9:
  - 8.9.2.1-WS-ODM_DS-IF004

Xehetasuna:

- IBM Operational Decision Manager-ek XML *External Entity Injection* (XXE) erako eraso bat jasan lezake XML datuak prozesatzean. Urruneko erasotzaile batek ahultasun hori balia lezake informazio sentikorra agerian uzteko edo memoriaren baliabideak kontsumitzeko. Ahultasun horretarako CVE-2018-1821 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Netgear-en produktuetan

Argitalpen data: 2018/12/14

Garrantzia: Handia

Kaltetutako baliabideak:

- D3600 eta D6000, firmwarearen 1.0.0.75 bertsioa baino lehenagokoak
- D6100, firmwarearen 1.0.0.58 bertsioa baino lehenagokoak
- D7800, firmwarearen 1.0.1.42 bertsioa baino lehenagokoak
- D8500, firmwarearen 1.0.3.42 bertsioa baino lehenagokoak
- EX3700 eta EX3800, firmwarearen 1.0.0.70 bertsioa baino lehenagokoak
- EX6000, firmwarearen 1.0.0.30 bertsioa baino lehenagokoak
- EX6100, firmwarearen 1.0.2.24 bertsioa baino lehenagokoak
- EX6120, firmwarearen 1.0.0.40 bertsioa baino lehenagokoak
- EX6130, firmwarearen 1.0.0.22 bertsioa baino lehenagokoak
- EX6150, 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
- EX6100v2 eta EX6150v2, firmwarearen 1.0.1.70 bertsioa baino lehenagokoak
- EX6200v2, firmwarearen 1.0.1.64 bertsioa baino lehenagokoak
- EX6400 eta EX7300, firmwarearen 1.0.2.136 bertsioa baino lehenagokoak
- R6100, firmwarearen 1.0.1.16 bertsioa baino lehenagokoak
- R6250, firmwarearen 1.0.4.26 bertsioa baino lehenagokoak
- R6300-2CXNAS, firmwarearen 1.0.3.60 bertsioa baino lehenagokoak
- R6300v2, firmwarearen 1.0.4.28 bertsioa baino lehenagokoak
- R6400, firmwarearen 1.0.1.36 bertsioa baino lehenagokoak

- R6400v2, firmwarearen 1.0.2.52 bertsioa baino lehenagokoak
- R6700 eta R6900, firmwarearen 1.0.1.46 bertsioa baino lehenagokoak
- R7000, firmwarearen 1.0.9.28 bertsioa baino lehenagokoak
- R7100LG, firmwarearen 1.0.0.46 bertsioa baino lehenagokoak
- R7300, firmwarearen 1.0.0.68 bertsioa baino lehenagokoak
- R7500, firmwarearen 1.0.0.110 bertsioa baino lehenagokoak
- R7500v2, firmwarearen 1.0.3.36 bertsioa baino lehenagokoak
- R7800, firmwarearen 1.0.2.32 bertsioa baino lehenagokoak
- R7900, firmwarearen 1.0.2.10 bertsioa baino lehenagokoak
- R8000, firmwarearen 1.0.4.18 bertsioa baino lehenagokoak
- R8900 eta R9000, firmwarearen 1.0.4.12 bertsioa baino lehenagokoak
- R8300 eta R8500, firmwarearen 1.0.2.122 bertsioa baino lehenagokoak
- R6900P eta R7000P, firmwarearen 1.3.1.44 bertsioa baino lehenagokoak
- R7900P eta R8000P, firmwarearen 1.3.0.10 bertsioa baino lehenagokoak
- WAC120, firmwarearen 2.1.7 bertsioa baino lehenagokoak
- WAC505 eta WAC510, firmwarearen 5.0.5.4 bertsioa baino lehenagokoak
- WNAP320, WNAP210v2, WNDAP350, WNDAP360 eta WNDAP660, firmwarearen 3.7.11.4 bertsioa baino lehenagokoak
- WNDAP620, firmwarearen 2.1.7 bertsioa baino lehenagokoak
- WND930, firmwarearen 2.1.5 bertsioa baino lehenagokoak
- WN604, firmwarearen 3.3.10 bertsioa baino lehenagokoak
- WN2500RPv2, firmwarearen 1.0.0.54 bertsioa baino lehenagokoak
- WN3000RPv2 eta WNR3500Lv2, firmwarearen 1.2.0.56 bertsioa baino lehenagokoak
- WN3000RPv3, firmwarearen 1.0.2.52 bertsioa baino lehenagokoak
- WNDR3700v4, firmwarearen 1.0.2.102 bertsioa baino lehenagokoak
- WNDR4300, firmwarearen 1.0.2.104 bertsioa baino lehenagokoak
- WNDR4300v2 eta WNDR4500v3, firmwarearen 1.0.0.50 bertsioa baino lehenagokoak
- WNR2000v5, firmwarearen 1.0.0.66 bertsioa baino lehenagokoak
- ReadyNAS OS 6, firmwarearen 6.9.3 bertsioa baino lehenagokoak
- SRR60 eta SRS60, firmwarearen 2.2.1.210 bertsioa baino lehenagokoak

Azalpena:

Netgear-ek 22 ahultasunen berri eman du, horietatik 6 larritasun altukoak.

Konponbidea:

- Firmwarearen azken bertsiora eguneratzea, beraien deskargen zentroan eskuragarri.

Xehetasuna:

Ahultasun horietako batzuk arrakastaz baliatuz gero, ondokoak eragin litezke:

- Komandoen injekzioa autentifikazioaren aurretik.
- Komandoen injekzioa autentifikazioaren ondoren.
- Cross-site request forgery.
- Cross-site Scripting.
- Haririk gabeko sarbide puntuetan segurtasunaren konfigurazio okerra.
- Pilaren gainezkatzea autentifikazioaren aurretik.
- Pilaren gainezkatzea autentifikazioaren ondoren.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna F5en hainbat produktutan

Argitalpen data: 2018/12/17

Garrantzia: Handia

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator)
  - 14.0.0tik 14.1.0ra bitarteko bertsioak
  - 13.1.0tik 13.1.1era bitarteko bertsioak
- BIG-IQ Centralized Management
  - 6.0.0tik 6.0.1era bitarteko bertsioak
  - 5.2.0tik 5.4.0ra bitarteko bertsioak

Azalpena:

Urruneko erasotzaile batek ordenagailu bat konekta lezake arazketa atakara eta JavaScript arbitrario bat exekutatu.

Konponbidea:

- BIG-IQ Centralized Management-en kasuan, 6.0.0tik 6.0.1era bitarteko bertsioak, 6.1.0 bertsiora eguneratu.
- Gainerako produktu eta bertsioen kasuan oraingoz ez da eguneraketarik argitaratu. Ahultasun hau nola arindu F5en orrialdean ikus daiteke, *Erreferentziak* atalean argitaratuta dago.

Xehetasuna:

- F5en iRulesLX osagaiak erabiltzen duen Node.js-ri eragiten dion ahultasun bat baliatuz (6.15.0 baino lehenagoko bertsioak), edozein interfazetan modu lehenetsian arazteko erabiltzen den 5858 atakara konekta liteke urruneko erasotzaile bat eta JavaScript arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2018-12120 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioen eskalatze erako ahultasuna VMWare-ren vRealize Operations-en

Argitalpen data: 2018/12/19

Garrantzia: Handia

Kaltetutako baliabideak:

- VMWare vRealize Operations (vROps), honako bertsioak:
  - 7.x
  - 6.7.x
  - 6.6.x

Azalpena:

Alessandro Zanni ikertzaileak, OVHko *pentester*-a, pribilegio lokalen eskalatze erako ahultasun bat aurkitu du.

Konponbidea:

Kaltetutako bertsioaren arabera, ordeztea edo dagokion partxea aplikatzea:

- vRealize Operations 7.0.0.11287810
- vRealize Operations 6.7.0.11286837
- vRealize Operations 6.6.1.11286876

Xehetasuna:

- vROps-ek pribilegio lokalen eskalatze erako ahultasun bat dauka, laguntzako *script*-en baimen desegoki batzuk direla eta. Terminalera sarbidea duen vROPS aplikazioaren erabiltzaile *administratzaileak* arazo hau balia lezake *root* pribilegioak igotzeko vROPS makina batean. Ahultasun horretarako CVE-2018-6978 identifikatzailea erabili da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Pribilegioen eskalatze ahultasuna Cisco Adaptative Security Appliance-n (ASA)

Argitalpen data: 2018/12/20

Garrantzia: Handia

Kaltetutako baliabideak:

- ASA softwarea exekutatzen duten eta web administrazioaren sarbidea gaituta duten Cisco produktu guztiak.

Azalpena:

Cisco Adaptative Security Appliance-k (ASA) duen pribilegioen eskalatze ahultasun baten berri eman du Ciscok.

Konponbidea:

Ciscok eguneratzea edo bertsioz aldatzea gomendatzen du:

- 9.3 baino lehenagoko bertsioen kasuan, 9.4.4.29 bertsiora migratzea
- 9.4 bertsioaren kasuan, 9.4.4.29 bertsiora eguneratzea
- 9.5 bertsioaren kasuan, 9.6.4.20 bertsiora migratzea
- 9.6 bertsioaren kasuan, 9.6.4.20 bertsiora eguneratzea
- 9.7 bertsioaren kasuan, 9.8.3.18 bertsiora migratzea
- 9.8 bertsioaren kasuan, 9.8.3.18 bertsiora eguneratzea
- 9.9 bertsioaren kasuan, 9.9.2.36 bertsiora eguneratzea
- 9.10 bertsioaren kasuan, 9.10.1.7 bertsiora eguneratzea

Softwarea beren deskarga zentroan eskura daiteke.

Xehetasuna:

- Web administrazioaren interfazea erabiltzean erabiltzaileen pribilegioen baliozkotze oker bat baliatuz, autentifikatutako baina pribilegiorik gabeko urruneko erasotzaile batek ekintza pribilegiatuak egin litzake interfaze hori erabiliz. Ahultasun horretarako CVE-2018-15465 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun IBMren produktuetan

Argitalpen data: 2018/12/20

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM Domino, 9.0.1etik 9.0.1 FP10 IF4ra bitarteko bertsioak eta 9.0tik 9.0 IF4ra bitartekoak
- IBM Notes, 9.0.1etik 9.0.1 FP10 IF5era bitarteko bertsioak eta 9.0tik 9.0 IF4ra bitartekoak
- IBM API Connect, 2018.1etik 2018.4.1era bitarteko bertsioak eta 5.0.0.0tik 5.0.8.4ra bitartekoak

Azalpena:

IBMk Domino, Notes eta API Connect bere produktuei eragiten dieten hainbat ahultasunen berri eman du. Horiek baliatuz pribilegioen eskalatzea, autentifikazioa saihestea, NoSQL injekzioa eta baimen propioak eskalatzea lor liteke.

Konponbidea:

- IBM Domino 9.0.1 FP10IF5en kasuan, behin behineko ohar teknikoa hau irakurri.

- IBM Notes Standard 9.0.1 FP10IF6ren kasuan, Fix Central ID Notes_901FP10IF6_W32_Standard deskargatu.
- IBM Notes Basic 9.0.1 FP10IF6ren kasuan, Fix Central ID Notes_901FP10IF6_W32_Basic deskargatu.
- IBM API Connect-en kasuan, dagokionaren arabera 2018.4.1.1 edo 5.0.8.5 bertsioak deskargatu.

Xehetasuna:

- IBM Notes-ek eta Domino-k (Windowsen soilik) pribilegioen eskalatze erako ahultasun bat daukate. Partekatutako memoriaren IPCaren bidez bidalitako komandoen lerro bat sortzean, *Notes System Diagnostic* (NSD) zerbitzua engaina daiteke, erasotzaileak aukeratutako *dll* fitxategi gaizto bat exekuta dezan. Ahultasun horretarako CVE-2018-1771 identifikatzailea erreserbatu da.
- IBM LoopBack baliatuz, erasotzaile batek autentifikazioa saihets lezake *AccessToken* modeloa API REST baten bidez jartzen bada agerian. Izan ere, posible da *AccessToken* bat sortzea edozein erabiltzailerentzat, bere erabiltzaile IDa ezagutuz gero. Horrela, beraz, gainerako erabiltzaileen datuetara edo euren pribilegioetara sarbidea lor liteke. Ahultasun horretarako CVE-2018-1778 identifikatzailea erreserbatu da.
- LoopBack frameworkerako MongoDB konektoreko NoSQL injekzio batek IBM API Connect-i eragiten dio. Ahultasun horretarako CVE-2018-1784 identifikatzailea erreserbatu da.
- API Connect V5ek *API Administrator*-en mailara sarbide mugatua duen erabiltzaile bati ahalbidetzen dio bere buruari sarbide osoa ematea *Administrator* mailara, kideen funtzionaltasunaren bidez. Ahultasun horretarako CVE-2018-1973 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Memoriaren hondatze erako ahultasuna Microsoft-en Internet Explorer-en

Argitalpen data: 2018/12/20

Garrantzia: Handia

Kaltetutako baliabideak:

- Internet Explorer 9, 10 eta 11

Azalpena:

Microsoftek zikloz kanpoko ohartarazpen bat argitaratu du kodearen urruneko exekuzioaren erakoa, Internet Explorer-en memoriako objektuak maneiatzean *scripting*-aren motorrak kudeaketan egiten duen akats baten ondorioz.

Konponbidea:

- Microsoftek oraingoz ez du aurkitu konponbide bat ahultasun horretarako.
- Arintze neurri modura, Carnegie Mellon University-k hainbat babes neurri argitaratu ditu.

Xehetasuna:

- Ahultasun hori arrakastaz baliatuz gero, erasotzaile batek memoria honda lezake, eta ondorioz oraingo erabiltzailearen testuinguruan kode arbitrarioa exekuta liteke edo erabiltzaile horren pribilegio berdinak eskuratu. Administratzaile pribilegioak lortuz gero, erasotzaileak programak instala litzake, datuak ikusi, aldatu edo ezabatu litzake, edo kontu berriak sor litzake administratzaile pribilegioekin. Ahultasun horretarako CVE-2018-8653 identifikatzailea erreserbatu da.

Etiketak: Microsoft, Nabigatzailea, Ahultasuna

Fitxategien txertatze ahultasuna Kibana-n

Argitalpen data: 2018/12/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Kibana, 6.4.3 eta 5.6.13 baino lehenagoko bertsioak

Azalpena:

Kibanak LFI (*Local File Inclusion*) prozesuan duen ahultasun baten berri argitaratu da. Ahultasun horrek fitxategiak txertatzea ahalbidetu lezake http eskaeren bidez.

Konponbidea:

- 6.5 bertsiora eguneratzea.

Xehetasuna:

- Kibanaren kontsolaren APIaren bitartez, Kibanak baimenak dituen zerbitzariaren edozein direktoriotan gordeta dauden Java Script fitxategiak exekutatzea ahalbidetuko liokeen http eskaera bat bidal lezake erasotzaile batek. Horrela informazioa eskura lezake eta makinaren kontrola lortzeko fitxategiak txertatzen utziko lioketen komandoak exekuta litzake. Ahultasun horretarako CVE-2018-17246 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun WIBU-SYSTEMS produktuetan

Argitalpen data: 2018/12/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- WibuKey.sys, 6.40 bertsioa (Build 2400)
- WibuKey Network zerbitzarien administratzailea, 6.40.2402.500 bertsioa

Azalpena:

Cisco Talos-eko Marcin 'Icewall' Noga ikertzaileak bi ahultasun aurkitu ditu WibuKey.sys produktuan, bat *kernel*aren memoriaren informazioaren zabalkunde erakoa eta bestea *pool*aren hondatzeagatik pribilegioen eskalatze erakoa. Bestalde, WibuKey Network produktuan beste ahultasun bat aurkitu du kodearen urruneko exekuzioaren erakoa.

Konponbidea:

- *WibuKey for Users*-en azken bertsioa jaistea software zentrotik.

Xehetasuna:

- Bereziki diseinatutako IRP eskaera batek eragin lezake hasieratu gabeko memoria itzultzea kontrolatzaileak, eta ondorioz *kernel*aren memoriaren informazioaren zabalkundea gertatuko litzateke. Ahultasun horretarako CVE-2018-3989 identifikatzailea erreserbatu da.
- Bereziki diseinatutako IRP eskaera batek bufferraren gainezkatzea eragin lezake eta ondorioz *kernel*aren memoria hondatzea gertatuko litzateke. Ahultasun horretarako CVE-2018-3990 identifikatzailea erreserbatu da.
- Bereziki diseinatutako TCP pakete batek *heap*aren gainezkatzea eragin lezake eta urruneko kodea exekutatzea ahalbidetu lezake *kernel* mailan. Ahultasun horretarako CVE-2018-3991 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Wi-Fi kredentzialen ihesa Orange-ren Livebox routerretan

Argitalpen data: 2018/12/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Livebox Arcadyan ARV7519RW22-A-L T VR9 1.2

Azalpena:

Bad Packets LLCko Troy Mursch segurtasun ikertzaileak ahultasun baten berri eman du. Hori baliatuz urruneko erasotzaile batek Livebox 2.1 routerren barne sareko Wi-Fi pasahitza eta SSID eskura litzake.

Konponbidea:

- Orange Livebox Arcadyan ARV7519 modemaren *firmware*ari, 00.96.00.96.96.613E bertsioa, akats horren aurkako partxe bat egin zaio.

Xehetasuna:

- Orange Livebox 00.96.320S gailuek duten ahultasun bat baliatuz, urruneko erasotzaile batek Wi-Fi kredentzialak eskura litzake */get_getnetworkconf.cgi* erako GET eskari bat eginez 8080 atakan. Horrela erabateko kontrola lortuko luke administratzailearen pasahitza Wi-Fi pasahitzaren berdina bada, edo administratzailearen balioa lehenetsia baldin badauka. Ahultasun horretarako CVE-2018-20377 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna