
# 2018ko Urriaren Bulletina

## Ohartarazpenak - Teknikoak

## Hainbat ahultasun Edge Caching Proxyk IBMren WebSphere Application Server-en erabilitako GSKit-en

**Argitalpen data:** 2018/10/03

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

Edge Caching Proxyren instalazio indibiduala, WebSphere Application Server-en bertsio hauetan:

- 9.0 bertsioa
- 8.5 bertsioa
- 8.0 bertsioa

**Azalpena:**

IBMk 7 ahultasun aurkitu ditu, 1 larritasun altukoa eta 6 larritasun ertain edo baxukoak.

**Konponbidea:**

IBMk ondoko konponbideak eskaini ditu:

- 9.0.0.0tik 9.0.0.8ra bitarteko bertsioen kasuan
  - Behin behineko 9.0.8 partxea aplikatzea edo
  - 9. partxea (v.9.0.0.9) edo goragokoa aplikatzea
- 8.5.0.0tik 8.5.5.14ra bitarteko bertsioen kasuan
  - Behin behineko 8.5.5 partxea aplikatzea edo
  - 15. partxea (v.8.5.5.15) edo goragokoa aplikatzea
- 8.0.0.0tik 8.0.0.15era bitarteko bertsioen kasuan
  - Behin behineko 8.0.0 partxea aplikatzea

**Xehetasuna:**

Larritasun altuko ahultasuna ondokoa da:

- IBM GSKit-ek (Linux, UNIX eta Windowserako IBM DB2) PRNG egoera bikoiztu egiten du fork() sisteman egindako deien bidez hainbat ICC instantzia kargatzen direnean. Honek eragin lezake saio ID bikoiztuak egotea edo material funtsezkoa bikoizteko arriskua sortzea. Ahultasun horretarako CVE-2018-1426 identifikatzailea erabili da.

Gainerako ahultasunetarako honako identifikatzaileak erabili dira: CVE-2018-1447, CVE-2018-1427, CVE-2017-3736, CVE-2017-3732, CVE-2016-0705 eta CVE-2016-0702.

**Etiketak:** Eguneraketa, IBM, Ahultasuna

## Hainbat ahultasun Cisco produktuetan

**Argitalpen data:** 2018/10/04

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Cisco PI Software, 3.2tik 3.4ra bitarteko bertsioak, zabaldutako lehen bertsioa baino lehenagokoak TFTP zerbitzaria gaituta baldin badago (lehenespenez hala egoten da).

- Cisco DNA Center, 1.1 bertsioa.
- Cisco DNA Center Software, 1.1.4 bertsioa baino lehenagokoak.
- Cisco Webex Business Suite:
  - WBS31: Cisco Webex Network Recording Player-en bertsio guztiak eta Cisco Webex Player-en WBS31.23 bertsioa baino lehenagokoak.
  - WBS32: Cisco Webex Network Recording Player-en bertsio guztiak eta Cisco Webex Player-en WBS32.15.20 bertsioa baino lehenagokoak.
  - WBS33: Cisco Webex Network Recording Player-en bertsio guztiak eta Cisco Webex Player-en WBS33.4 bertsioa baino lehenagokoak.
- Cisco Webex Meetings:
  - Online: Cisco Webex Network Recording Player-en bertsio guztiak eta 1.3.37 bertsioa baino lehenagokoak.
  - Server: Cisco Webex Network Recording Player-en 3.0MR2 Patch 1 bertsioa baino lehenagoko guztiak.
- Cisco SD-WAN Solution, 17.2.8 eta 18.3.1 bertsioak baino lehenagokoak, ondoko produktuetan exekutatzen direnean:
  - vBond Orchestrator Software.
  - vEdge 100 Series Routers.
  - vEdge 1000 Series Routers.
  - vEdge 2000 Series Routers.
  - vEdge 5000 Series Routers.
  - vEdge Cloud Router Platform.
  - vManage Network Management Software.
  - vSmart Controller Software.
- Cisco HyperFlex Software, 3.5(1a) bertsioa baino lehenagokoak.
- Cisco Firepower Threat Defense (FTD) Software, 6.2.3.4 baino lehenagoko 6.2.3.x bertsioak, FTP erregistroa gaituta baldin badago, FTP fitxategiko politika bat loturik duen sarbidearen kontrol arau bat ere gaituta badago eta softwarea ondoko produktuetakoren batean exekutatzen ari bada:
  - 3000 Series Industrial Security Appliances (ISAs).
  - ASA 5500-X Series Next-Generation Firewalls.
  - Firepower 2100 Series Security Appliances.
  - Firepower 4100 Series Security Appliances.
  - Firepower 9300 ASA Security Module.
  - Firepower Threat Defense Virtual (FTDv).
- Cisco Firepower System Software, ondoko produktuetakoren batean exekutatzen denean:
  - Adaptive Security Appliance (ASA) 5500-X Series, FirePOWER Services-ekin.
  - Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewalls.
  - Advanced Malware Protection (AMP) for Networks, 7000 eta 8000 Series Appliances.
  - Firepower 2100 eta 4100 Series Security Appliances.
  - FirePOWER 7000 eta 8000 Series Appliances.
  - Firepower 9300 Series Security Appliances.
  - FirePOWER Threat Defense for Integrated Services Routers (ISRs).
  - Firepower Threat Defense Virtual.
  - Industrial Ethernet 3000 Series Switches.
  - Next-Generation Intrusion Prevention System (NGIPSv).
  - Virtual Next-Generation Intrusion Prevention System (NGIPSv).
- Cisco Prime Collaboration Provisioning, 12.1 bertsioa baino lehenagokoak.
- Ondoko produktuak, baldin eta Cisco Adaptive Security Appliance (ASA) Software-ren edo Cisco Firepower Threat Defense (FTD) Software-ren bertsio ahul bat exekutatzen ari badira:
  - ASA 5506-X, FirePOWER Services-ekin.
  - ASA 5506H-X, FirePOWER Services-ekin.
  - ASA 5506W-X, FirePOWER Services-ekin.
  - ASA 5508-X, FirePOWER Services-ekin.
  - ASA 5516-X, FirePOWER Services-ekin.

**Azalpena:**

Ciscok bere hainbat produkturi buruzko 10 ahultasun argitaratu ditu, horietatik 3 larritasun kritikokoak eta 7 larritasun altukoak.

**Konponbidea:**

Ciscok erabiltzaileen eskura jarri ditu hainbat eguneraketa, kaltetutako produktuaren arabera.

- Software Ciscoren deskarga panela.

**Xehetasuna:**

Honakoak dira larritasun kritikoko ahultasunak:

- Cisco Prime Infrastructure-rako (PI) HTTP web zerbitzariak murrizpenik gabeko direktorio baimenak ditu. Hori baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek fitxategi arbitrario bat karga lezake eta komandoak exekuta litzake *prime* erabiltzailearen pribilegio mailan. Ahultasun horretarako CVE-2018-15379 identifikatzailea erreserbatu da.
- Cisco Digital Network Architecture (DNA) Center-ek duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek autentifikazioa saihets lezake eta administrazio funtzio kritikoetara baimenik gabeko sarbide zuzena lor lezake. Ahultasun horretarako CVE-2018-15386 identifikatzailea erreserbatu da.
- Cisco Digital Network Architecture (DNA) Center-en identitateen administrazio zerbitzuak duen ahultasun bat baliatuz, autentifikaziorik gabeko urruneko erasotzaile batek autentifikazioa saihets lezake eta identitateen administrazio funtzioen kontrol osoa har lezake. Ahultasun horretarako CVE-2018-0448 identifikatzailea erreserbatu da.

Kritikotasun altuko ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2018-15408, CVE-2018-15409, CVE-2018-15410, CVE-2018-15411, CVE-2018-15412, CVE-2018-15413, CVE-2018-15415, CVE-2018-15416, CVE-2018-15417, CVE-2018-15418, CVE-2018-15419, CVE-2018-15420, CVE-2018-15431, CVE-2018-15387, CVE-2018-15382, CVE-2018-15390, CVE-2018-0455, CVE-2018-15389 eta CVE-2018-15383.

**Etiketak:** Eguneraketa, Cisco, Ahultasuna

---

# Ahultasuna VMwareren AirWatch Console-n

**Argitalpen data:** 2018/10/08

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- AirWatch Console 9.7.x.

- AirWatch Console 9.6.x.
- AirWatch Console 9.5.x.
- AirWatch Console 9.4.x.
- AirWatch Console 9.3.x.
- AirWatch Console 9.2.x.
- AirWatch Console 9.1.x.

**Azalpena:**

SAMLen (Security Assertion Markup Language) autentifikaziorik ezaren moduko ahultasuna aurkitu da, gailuaren inskripzioaren unean baliatu daitekeena.

**Konponbidea:**

VMwarek produktuaren eguneratzea behar duten bertsioen zerrenda argitaratu du:

- AirWatch Console 9.7.0.3 edo goragokoa.
- AirWatch Console 9.6.0.7 edo goragokoa.
- AirWatch Console 9.5.0.16 edo goragokoa.
- AirWatch Console 9.4.0.22 edo goragokoa.
- AirWatch Console 9.3.0.25 edo goragokoa.
- AirWatch Console 9.2.3.27 edo goragokoa.
- AirWatch Console 9.1.5.6 edo goragokoa.

**Xehetasuna:**

VMware Workspace ONE Unified Endpoint Management Console-k (AirWatch Console) autentifikaziorik ezaren ahultasun bat dauka SAMLen (Security Assertion Markup Language), eta hori baliatu egin liteke gailua inskribatzean. Ahultasun hori baliatuz erasotzaile batek baimendutako SAML saio bat dela simula lezake, ziurtagirietan oinarritutako autentifikazioa gaituta baldin badago. Era berean, arriskua egon liteke ziurtagirietan oinarritutako autentifikazioa gaituta ez badago ere, baina kasu horietan ahultasuna baliatzearen emaitza informazioaren zabalkundera mugatuko litzateke. Ahultasun horretarako CVE-2018-6979 identifikatzailea erabili da.

**Etiketak:** Eguneraketa, VMware, Ahultasuna

---

# Hainbat ahultasun Central WiFi Manager produkturako D-Link-en

**Argitalpen data:** 2018/10/08

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- CWM-100: D-Link Central WiFi Manager, Windowserako 1.03 bertsioa

**Azalpena:**

D-Linkek Central WifiManager produktuari eragiten dioten 4 ahultasunen berri eman du (tresna honek sare baten barnean sarbide puntuak administratzea eta monitorizatzea ahalbidetzen du).

**Konponbidea:**

Ahultasun horiek konpontzeko D-Linkek 1.03 R0100 - Beta bertsiora eguneratzea aholkatzen du.

**Xehetasuna:**

Ahultasunak honakoak dira:

- Erasotzaile batek, autentifikazioaren beharrik gabe, fitxategi bat igo lezake eta urrunetik kode arbitrarioa exekutatu. Ahultasun horretarako CVE-2018-17440 identifikatzailea erreserbatu da.
- Autentifikatutako erasotzaile batek fitxategi bat igo lezake eta urrunetik kode arbitrarioa exekutatu. Ahultasun horretarako CVE-2018-17442 identifikatzailea erreserbatu da.
- Erasotzaile batek Cross-Site Scripting erako erasoak egin litzake "sitename" eta "addUser" parametroen bidez. Ahultasun horietarako CVE-2018-17441 eta CVE-2018-17443 identifikatzaileak erreserbatu dira.

**Etiketak:** Eguneraketa, Komunikazioak, Ahultasuna

---

# Pribilegioak eskalatzearen erako ahultasuna IBM Spectrum LSF-n

**Argitalpen data:** 2018/10/09

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- IBM Spectrum LSF, 10.1 bertsioa
- IBM Spectrum LSF, 9.1.1 bertsioa
- IBM Spectrum LSF, 9.1.2 bertsioa
- IBM Spectrum LSF, 9.1.3 bertsioa

**Azalpena:**

IBMk larritasun altuko ahultasun bat aurkitu du. Hori baliatuz erasotzaile batek pribilegioen eskalatzea lor lezake kaltetutako produktuetan.

**Konponbidea:**

IBMk kaltetutako produktuak bere deskarga zentrotik eguneratzea aholkatzen du.

**Xehetasuna:**

- IBMk Spectrum LSFk (Load Sharing Facility) zuen ahultasuna konpondu du "eauth" (kanpo autentifikazioa) fitxategi exekutagarria hobetuz, erabiltzailearen kredentzialak baimentzen dituena erasoak saihestearren "getuid" funtzioaren aurretiazko kargaren bitartez. Ahultasun horretarako CVE-2018-1724 identifikatzailea erreserbatu da.

**Etiketak:** Eguneraketa, IBM, Ahultasuna

---

# 2018ko urriko Microsoften segurtasun buletina

**Argitalpen data:** 2018/10/10

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office eta Microsoft Office Services eta Web Apps.
- ChakraCore
- . NET Core
- PowerShell Core
- SQL Server Management Studio
- Microsoft Exchange Server
- Azure IoT Edge
- Hub Device Client SDK for Azure IoT

**Azalpena:**

Segurtasun eguneraketei buruzko Microsoften hileroko argitalpenean 48 ahultasun jaso dira oraingoan; 12 kritiko gisa sailkatu dira eta 36 garrantzitsu gisa. Gainerakoak larritasun ertain edo baxukoak dira.

**Konponbidea:**

Dagozkien segurtasun eguneraketak instalatzea. Eguneraketen beraien instalaziorako informazio orrialdean hori egiteko metodo ezberdinei buruzko informazioa dago.

**Xehetasuna:**

Argitaratutako ahultasun motak ondokoak dira:

- Kodearen urrutiko exekuzioa.
- Informazioa ezagutaraztea.
- Pribilegioen igoera.
- Segurtasunari ihes egitea.

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

---

# Hainbat ahultasun Intel produktuetan

**Argitalpen data:** 2018/10/10

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Windowserako Intel® RAID Web Console, 3. bertsioa eta lehenagokoak
- Intel® NUC Firmware Kits, 2018ko maiatzaren 24a baino lehen deskargatutakoa
- Intel® Graphics Drivers, 10.18.x.5056 (15.33.x.5056), 10.18.x.5057 (15.36.x.5057) eta 20.19.x.5058 (15.40.x.5058) bertsioak baino lehenagokoak
- Intel® Client NVMe, 4.0.0.1006 bertsioa eta lehenagokoak.
- Datacenter NVMe, 4.0.0.1006 bertsioa eta lehenagokoak.
- Intel® RSTe, 4.7.0.2082 bertsioa eta lehenagokoak.
- Intel® Server Board S7200AP Family, R01.03.0018 baino lehenagoko firmware bertsioak.
- Intel® Compute Module HNS7200AP Family, R01.03.0018 baino lehenagoko firmware bertsioak.
- Intel® Server Board S7200APR Family, R01.03.0018 baino lehenagoko firmware bertsioak.
- Intel® Compute Module HNS7200APR Family, R01.03.0018 baino lehenagoko firmware bertsioak.

Firmwarearen 00.01.0014 bertsioa baino lehenagokoa duten produktu hauek ere kaltetuta daude:

- Intel® Server Board S2600BP Family
- Intel® Compute Module HNS2600BP Family
- Intel® Server System H2000G Family
- Intel® Server Board S2600WF Family
- Intel® Server System R2000WF Family
- Intel® Server System R1000WF Family
- Intel® Server Board S2600ST Family
- Intel® Server Board S2600BPR Family
- Intel® Compute Module HNS2600BPR Family
- Intel® Server System H2000GR Family
- Intel® Server Board S2600WFR Family
- Intel® Server System R2000WFR Family
- Intel® Server System R1000WFR Family
- Intel® Server Board S2600STR Family

**Azalpena:**

Intelek bere produktu batzuei eragiten dieten hainbat ahultasun argitaratu ditu, larritasun ertain eta altukoak.

**Konponbidea:**

Kaltetutako produktuak webgune honetatik eguneratu: https://downloadcenter.intel.com/es.

**Xehetasuna:**

Argitaratutako ahultasunetako batzuk balia litzake erasotzaile batek ondoko ekintzetako batzuk egin ahal izateko:

- Pribilegioen eskalatzea
- Zerbitzua ukatzea
- Informaziorako sarbidea baimenik gabe

Aipatutako ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2018-12173, CVE-2018-12161, CVE-2018-12158, CVE-2018-12152, CVE-2018-12153, CVE-2018-12154, CVE-2018-12131 eta CVE-2018-12172.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Zerbitzuaren ukapen erako ahultasuna VMware-n

**Argitalpen data:** 2018/10/10

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- VMware vSphere ESXi (ESXi), edozein plataformatarako edozein bertsio.
- VMware Workstation Pro / Player (Workstation), edozein plataformatarako edozein bertsio.
- VMware Fusion Pro, Fusion (Fusion), OS Xerako edozein bertsio.

**Azalpena:**

VMware ESXi, Workstation eta Fusion-ek zerbitzuaren ukapen erako ahultasun bat daukate, 3D renderizatuko iluntzaile batek duen begizta infinitu bat dela eta.

**Konponbidea:**

VMwarek ez du argitaratu inolako partxerik arazoa konpontzeko, eta 3Dren azeleratze funtzioa ezgaitzea aholkatzen du.

- ESXi-k ez dauka gaituta modu lehenetsian.
- Workstationek eta Fusionek modu lehenetsian gaituta daukate.

**Xehetasuna:**

- VMware ESXi, Workstation eta Fusionek zerbitzuaren ukapen erako ahultasun bat daukate, 3D renderizatuko iluntzaile batek duen begizta infinitu baten ondorioz. Hori baliatuz erasotzaile batek bereziki diseinatuta dagoen fitxategi iluntzaile bat gehi lezake (bai modu binarioan, bai testuan) hura aktibatzeko. Ahultasun hori sor daiteke VMwareren gonbidatutik, eta hortaz VMwareren hosta kalteturik aurkituko litzateke (eta horren ondorioz *vmware-vmx.exe* blokeatu egingo litzateke hostean). Ahultasun horretarako CVE-2018-6977 identifikatzailea erabili da.

**Etiketak:** VMware, Ahultasuna

---

# SAPen segurtasun eguneraketa 2018ko urria

**Argitalpen data:** 2018/10/10

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- SAP BusinessObjects Business Intelligence Platform, 4.1 eta 4.2 bertsioak.
- SAP Business Client, 6.5 bertsioa.
- Proyecto Gardener, 0.12.2 bertsioa.
- SAP Plant Connectivity, 15.0, 15.1 eta 15.2 bertsioak.
- SAP Records Management, 7.0tik 7.02ra bitarteko bertsioak, eta 7.10, 7.11, 7.30, 7.31, 7.40, 7.50 eta 7.51.
- SAP HANA, 1.0 eta 2.0 bertsioak.
- ABABerako SAP Netweaver Application Server, 7.0tik 7.02ra bitarteko bertsioak, 7.30, 7.31, 7.40, eta 7.50tik 7.53ra.
- SAP BusinessObjects Business Intelligence Platform, 4.10 eta 4.20 bertsioak.
- SAP Data Services, 4.2 bertsioa.
- SAP Plant Connectivity, 15.0 bertsioa.
- SAP BusinessObjects BI Platform Servers (Software Development Kit), 4.1 eta 4.2 bertsioak.
- SAP Adaptive Server Enterprise (ASE), 15.7 eta 16.0 bertsioak.
- SAP Fiori 1.0, SAP ERP HCMrako (Approve Leave Request, 2. bertsioa), 1.0 bertsioa.
- SAP Fiori 1.0, SAP ERP HCMrako (Approve Leave Request, 2. bertsioa), 1.0 bertsioa.
- SAP Adaptive Server Enterprise (ASE), 15.7 eta 16.0 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 15 segurtasun ohar eman ditu ezagutzera. Horietatik 4 ohar lehenagotik argitaratutako segurtasun oharrei dagozkien eguneraketak dira (horietako bat larritasun kritikokoa, 2 larritasun altukoak eta

bat larritasun ertainekoa), 1 larritasun kritikokoa da, beste 2 larritasun altukoak eta beste 8 larritasun ertainekoak.

Argitaratutako ahultasun motak ondokoak dira:

- Informazio zabalkundeko 3 ahultasun.
- Chromium nabigatzailearen kontrolerako segurtasun eguneraketen ahultasun bat.
- Sarearen isolamendu okerreko ahultasun bat.
- Zerbitzuaren ukazioko ahultasun bat.
- Pribilegioen aprobetxamenduko ahultasun bat.
- XMLren balioztatze okerreko 2 ahultasun.
- Cross-Site Scripting erako 3 ahultasun.
- Fitxategiaren bidearen zabalkunde erako ahultasun bat.
- Cross-Site Request Forgery erako 2 ahultasun.

Ahultasun garrantzitsuenak ondokoak dira:

- SAP BusinessObjects BI Suite-k informazioaren zabalkunde erako ahultasun bat dauka. Erasotzaile batek informazio gehigarria (sistemaren datuak, depurazio informazioa eta abar) ezagutarazteko erabil dezake, horrek sistema ezagutzen lagunduko lioke eta beste eraso batzuk antola litzake. Ahultasun horretarako CVE-2018-2471 identifikatzailea erabili da.
- Gardener proiektuak sarearen isolamendu okerreko ahultasun bat dauka eta horrek erasotzaile bati ahalbidetuko lioke, *shoot cluster* batean administratzaile modura jokatuz gero, dagokion *seed cluster-a* edo *seed cluster* horrek kontrolatzen dituen beste *seed cluster* batzuk arriskuan jartzea. Ahultasun horretarako CVE-2018-2475 identifikatzailea erabili da.
- SAP Plant Connectivity-k (PCo) zerbitzuaren ukapen (DoS) erako ahultasun bat dauka. Horrek erasotzaile bati ahalbidetuko lioke kaltetutako osagaiaren prozesu bat amaitzea. Ahultasun horietarako CVE-2018-12585 eta CVE-2018-12086 identifikatzaileak erabili dira.

SAPen 2018ko urriko hileko txostenean ageri diren gainerako CVE identifikatzaileak honakoak dira: CVE-2018-2465, CVE-2018-2470, CVE-2018-2472, CVE-2018-2466, CVE-2017-12069, CVE-2018-2467, CVE-2018-2469, CVE-2018-2474, CVE-2018-2474 eta CVE-2018-2468.

**Etiketak:** Eguneraketa, SAP, Ahultasuna

---

# Segurtasun eguneraketa Joomla! 3.8.13n

**Argitalpen data:** 2018/10/10

**Garrantzia:** Txikia

**Kaltetutako baliabideak:**

- Joomla! CMS, 1.5.0tik 3.8.12ra bitarteko bertsioak

**Azalpena:**

Joomlak bere CMSaren eguneraketa bat argitaratu du hainbat ahultasun konpontzen dituena. Horiek baliatuz, erasotzaile batek CSFR bat egin lezake, *admin* pribilegioak behar dituzten eguneraketak egin litzake edo baimendu gabeko sarbide maila bat eskuratu.

**Konponbidea:**

Joomla!-ren 3.8.13 bertsiora eguneratu.

**Xehetasuna:**

Konpondutako ahultasunak honakoak dira, guztiak Joomla!-ren nukleoan:

- *com_installer*-en CSRFren aurkako babesa
- ACLren bortxaketa *com_users*-en administratzailearen egiaztapen prozesuan
- Sarbide mailaren bortxaketa *com_tags*-en
- Lehenetsitako sarbide maila okerra *com_joomlaupdate*-rako
- *com_contact* kontaktuen inprimakiaren babesa

Aipatutako ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2018-17858, CVE-2018-17855, CVE-2018-17857, CVE-2018-17856 eta CVE-2018-17859.

**Etiketak:** Eguneraketa, Edukien kudeatzailea, Ahultasuna

---

# Hainbat ahultasun Juniper produktuetan

**Argitalpen data:** 2018/10/11

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Junos OS, hainbat bertsio (xehetasunetarako ikusi *Erreferentziak* atala)
- Junos Space Network Management Platform, 18.2R1 baino lehenagoko bertsioak
- Junos Space Security Director, 17.2R1 baino lehenagoko bertsioak

**Azalpena:**

Juniper-ek bere hainbat produkturi buruzko 15 ahultasunen berri eman du, horietatik 10 larritasun altukoak eta 5 larritasun ertainekoak.

**Konponbidea:**

Kaltetutako produktuak webgune honetatik eguneratu:

- https://www.juniper.net/support/downloads/

**Xehetasuna:**

Larritasun altuko ahultasunek ondorio hauek izan dezakete:

- **Urruneko sarbidea baimenik gabe.** Identifikatzaile hau duen ahultasunerako: CVE-2018-0044.
- **Informazio lapurreta.** Identifikatzaile hau duen ahultasunerako: CVE-2018-0047.
- **Cross-site Scripting**. Identifikatzaile hau duen ahultasunerako: CVE-2018-0046.
- **Zerbitzua ukatzea.** Identifikatzaile hauek dituzten ahultasunetarako: CVE-2018-0043, CVE-2018-0045, CVE-2018-0048, CVE-2018-0049, CVE-2018-0050, CVE-2018-0051 eta CVE-2018-0052.

Gainerako ahultasunetarako honako identifikatzaileak erabili dira: CVE-2018-0053, CVE-2018-0054, CVE-2018-0055, CVE-2018-0056 eta CVE-2018-0057.

**Etiketak:** Eguneraketa, Sistema Eragilea, Ahultasuna

---

# Hainbat ahultasun IBM Cloud-en IBM WebSphere Application Server-en

**Argitalpen data:** 2018/10/11

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

Ahultasun honek IBM WebSphere Application Server-en ondoko bertsioei eragiten die:

- Liberty
- 9.0 bertsioa
- 8.5 bertsioa

**Azalpena:**

IBMk segurtasun buletin bat argitaratu du IBM Cloud-eko IBM WebSphere Application Server-i eragiten dioten hainbat ahultasunen berri emanez.

**Konponbidea:**

Existitzeen den zerbitzu instantzia bat zuzentzeko, segurtasun buletineko *Remediation/Fixes* atalean zerrendatuta agertzen den ahultasun zehatzari buruzko ohartarazpena ireki beharra dago, eta bertan azalduta agertzen diren urratsak eman. Edo bestela, kaltea duen zerbitzuaren instantzia ezabatu beharra dago, eta instantzia berri bat sortu.

**Xehetasuna:**

Azaldutako ahultasunak honakoak dira:

- IBM WebSphere Application Server-ek urruneko erasotzaile bati ahalbidetu liezaioke Java kode arbitrarioa exekutatzen SOAP (*Simple Object Access Protocol*) konektorearen bidez, iturri ez fidagarriko objektu serializatu batekin. Ahultasun horretarako CVE-2018-1567 identifikatzailea erabili da.
- Apache MyFaces eta Oracle Mojarra baliatuz urruneko erasotzaile batek sisteman kode arbitrarioa exekuta lezake, ViewStateren konfigurazio oker baten eraginez. ViewState konfiguratuta badago egoeraren informazio ez zifratua erabiltzeko, erasotzaile batek ahultasun hori balia lezake zerbitzariaren *classpath*-ean dagoen edozein kode exekutatzeko.
- *Form Login* erabiltzen duten IBM WebSphere Application Server-en instalazioek urruneko erasotzaile bati ahalbidetu liezaiokete *spoofing* erasoak egitea. Ahultasun horretarako CVE-2018-1695 identifikatzailea erabili da.
- IBM WebSphere Application Server-ek baldintza jakin batzuetan espero litekeena baino segurtasun ahulagoa eskain lezake. Horren ondorioz TLS protokoloaren downgrade erako eraso bat gerta liteke. Urruneko erasotzaile batek ahultasun hori balia lezake *man-in-the-middle* erasoak egiteko. Ahultasun horretarako CVE-2018-1719 identifikatzailea erabili da.
- WebSphere Application Server Liberty-k urruneko erasotzaile bati informazio konfidentziala eskuratzea ahalbidetu liezaioke, garraio oker batek eraginda Liberty konfiguratuta dagoenean JASPIC (*Java Authentication SPI for Containers*) erabiltzeko. Hori gerta daiteke aplikazioen zerbitzaria konfiguratuta dagoenean ataka ez seguru batera (http) sarbidea baimentzeko JASPIC edo JSR375 autentifikazioa erabiliz. Ahultasun horretarako CVE-2018-1755 identifikatzailea erabili da.
- IBM WebSphere Application Server Liberty-k urruneko erasotzaile bati informazio konfidentziala eskuratzea ahalbidetu liezaioke, ORB (*Object Request Broker*) komunikazioaren enkriptazioak daukan akatsak eraginda. Ahultasun horretarako CVE-2018-1683 identifikatzailea erabili da.
- IBM Cloud-eko IBM WebSphere Application Server-ek urruneko erasotzaile bati informazio konfidentziala eskuratzea ahalbidetu liezaioke, pasahitzen erabilera oker baten eraginez. Ahultasun horretarako CVE-2018-1838 identifikatzailea erabili da.

**Etiketak:** Eguneraketa, IBM, Ahultasuna

---

# Hainbat ahultasun PHP-n

**Argitalpen data:** 2018/10/15

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- PHP, 7.2.x bertsioak
- PHP, 7.1.x bertsioak

**Azalpena:**

PHPren hainbat ahultasunen berri eman da, gorago aipatutako bertsioei dagozkienak.

**Konponbidea:**

PHP ondoko bertsio hauetako batera eguneratzea, instalatutako produktu adarraren arabera:

- PHP, 7.2.11 bertsioa
- PHP, 7.1.23 bertsioa

**Xehetasuna:**

Eguneraketek kaltetutako bertsioetako akatsak konpontzen dituzte, baita honako ahultasunak zuzendu ere:

- Salbuespen okerra *ReflectionMethod* erabiltzean.
- Sistema eragileak aldioro ezabatzea *ZendOPcache.MemoryBase*.
- *expat*-ekin (XMLren parser-a) *xmlrpc* ezin eraikitzea.
- Memoria mugen akats baten ondoren, itzaltzeko funtzioan segmentu akatsa.
- *posix_getgrnam*-ek taldearen xehetasunak ez inprimatzea.

**Etiketak:** Eguneraketa, PHP, Ahultasuna

---

# Hainbat ahultasun IBMren produktuetan

**Argitalpen data:** 2018/10/15

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- IBM Flex System Chassis Management Module (CMM), 2PET bertsioa,
- VRA - Vyatta 5600,
- FileNet Content Manager, 5.2.1 eta 5.5.0 bertsioak,
- IBM Flex System Chassis Management Module (CMM).

**Azalpena:**

IBMk bere produktuei eragiten dieten hainbat ahultasunen berri eman du, bat kritikoa, bost altuak eta bat ertaina. Horiek baliatuz informazio sentikorra eskura liteke, pribilegioak eskalatu, zerbitzuaren ukapena eragin edo memoria kontsumitu.

**Konponbidea:**

- IBM Flex System Chassis Management Module (CMM), 2PET bertsioaren, eta IBM Flex System Chassis Management Module-ren (CMM) kasuetan, eguneraketa hemen eskuratu: http://www.ibm.com/support/fixcentral/
- VRA - Vyatta 5600en kasuan, IBM Cloud Supportekin harremanetan jarri, 1801q releasearen ISOa zure Vyatta sistemara bidalia izan dadin eskatzeko.
- FileNet Content Manager, 5.2.1 eta 5.5.0 bertsioen kasuan, 5.2.1.7-P8CPE-IF004 edo 5.5.1.0-P8CPE bertsioak instalatu.

**Xehetasuna:**

- Apache Portable Runtime APRk duen ahultasunak IBM Flex System Chassis Management Module-ri eragiten dio eta hura baliatuz urruneko erasotzaile batek informazio sentikorra eskura lezake, apr_time_exp*() funtzioetan mugez kanpoko matrize bat erabiliz. Hilabetearen eremuan baliagarria ez den balio bat erabiliz, urruneko erasotzaile batek ahultasun hori balia lezake informazio konfidentziala eskuratzeko edo zerbitzuaren ukapen egoera sortzeko. Larritasun kritikoko ahultasun horretarako CVE-2017-12613 identifikatzailea erabili da.

Gainerako ahultasunetarako erreserbatutako identifikatzaileak honakoak dira: CVE-2018-13405, CVE-2018-5390, CVE-2018-3646, CVE-2018-3620, CVE-2018-1844 eta CVE-2017-17833.

**Etiketak:** Eguneraketa, IBM, Ahultasuna

---

# Eguneraketa kritikoak Oraclen (2018ko urria)

**Argitalpen data:** 2018/10/17

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Application Management Pack for Oracle E-Business Suite, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 bertsioak
- Enterprise Manager Base Platform, 12.1.0.5, 13.2 bertsioak
- Enterprise Manager for MySQL Database, 13.2 bertsioa
- Enterprise Manager Ops Center, 12.2.2, 12.3.3 bertsioak
- Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2 eta M12-2S Servers, XCP2352 eta XCP3050 baino lehenagoko bertsioak
- Hyperion BI, 11.1.2.4 bertsioa
- Hyperion Common Events, 11.1.2.4 bertsioa
- Hyperion Data Relationship Management, 11.1.2.4.345 bertsioa
- Hyperion Essbase Administration Services, 11.1.2.4 bertsioa
- Instantis EnterpriseTrack, 17.1, 17.2, 17.3 bertsioak
- JD Edwards EnterpriseOne Orchestrator, 9.2 bertsioa
- JD Edwards EnterpriseOne Tools, 9.2 bertsioa
- MICROS Lucas, 2.9.5 bertsioa
- MICROS PC Workstation 2015, 01.3.0.2i baino lehenagoko BIOS bertsioak
- MICROS Relate CRM Software, 10.8, 11.4 bertsioak
- MICROS Retail-J, 12.1.2, 13.0.0 bertsioak
- MICROS XBRi, 10.5.0, 10.6.0, 10.7.0, 10.8.1, 10.8.2, 10.8.3 bertsioak
- MySQL Connectors, 8.0.12 eta lehenagoko bertsioak
- MySQL Enterprise Monitor, 3.4.9.4237 bertsioa eta aurrekoak, 4.0.6.5281 eta aurrekoak, 8.0.2.8191 eta aurrekoak
- MySQL Server, 5.5.61 bertsioa eta aurrekoak, 5.6.41 bertsioa eta aurrekoak, 5.7.23 bertsioa eta aurrekoak, 8.0.12 bertsioa eta aurrekoak
- Oracle Adaptive Access Manager, 11.1.1.7.0, 11.1.2.3.0 bertsioak
- Oracle Agile Engineering Data Management, 6.1.3, 6.2.0, 6.2.1 bertsioak
- Oracle Agile PLM, 9.3.3, 9.3.4, 9.3.5, 9.3.6 bertsioak
- Oracle Agile Product Lifecycle Management for Process, 6.2.0.0 bertsioa
- Oracle API Gateway, 11.1.2.4.0 bertsioa
- Oracle Banking Platform, 2.5.0, 2.6.0, 2.6.1, 2.6.2 bertsioak
- Oracle BI Publisher, 11.1.1.7.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak
- Oracle Big Data Discovery, 1.6.0 bertsioa

- Oracle Business Intelligence Enterprise Edition, 11.1.1.7.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak
- Oracle Communications Application Session Controller, Prior to 3.7.1M0 bertsioak
- Oracle Communications Instant Messaging Server, prior to 10.0.1 bertsioak
- Oracle Communications Messaging Server, prior to 8.0.2 bertsioak
- Oracle Communications MetaSolv Solution, 6.3.0 bertsioa
- Oracle Communications Performance Intelligence Center (PIC) Software, prior to 10.2.1 bertsioak
- Oracle Communications User Data Repository, prior to 12.2.0 bertsioak
- Oracle Configuration Manager, 12.1.2.0.2, 12.1.2.0.5 bertsioak
- Oracle Database Server, 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c bertsioak
- Oracle Demantra Demand Management, 7.3.5, 12.2 bertsioak
- Oracle Directory Server Enterprise Edition, 11.1.1.7 bertsioa
- Oracle E-Business Suite, 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 bertsioak
- Oracle Endeca Information Discovery Integrator, 3.1.0, 3.2.0 bertsioak
- Oracle Endeca Information Discovery Integrator, 3.1.0, 3.2.0 bertsioak
- Oracle Endeca Server, 7.6.1, 7.7.0 bertsioak
- Oracle Enterprise Repository, 11.1.1.7.0, 12.1.3.0.0 bertsioak
- Oracle Fusion Middleware MapViewer, 12.1.3.0, 12.2.1.3 bertsioak
- Oracle GlassFish Server, 3.1.2 bertsioa
- Oracle GoldenGate, 12.1.2.1.0, 12.2.0.2.0, 12.3.0.1.0 bertsioa
- Oracle GoldenGate for Big Data, 12.2.0.1, 12.3.1.1, 12.3.2.1 bertsioak
- Oracle Healthcare Translational Research, 3.1.0 bertsioak
- Oracle Hospitality Cruise Fleet Management, 9.0 bertsioak
- Oracle Hospitality Cruise Shipboard Property Management System, 8.0 bertsioa
- Oracle Hospitality Gift and Loyalty, 9.0 bertsioa
- Oracle Hospitality Guest Access, 4.2.0, 4.2.1 bertsioak
- Oracle Hospitality Materials Control, 18.1 bertsioak
- Oracle Hospitality Reporting and Analytics, 9.0 bertsioa
- Oracle HTTP Server, 12.2.1.3 bertsioak
- Oracle Identity Analytics, 11.1.1.5.8 bertsioak
- Oracle Identity Management Suite, 11.1.2.3.0, 12.2.1.3.0 bertsioak
- Oracle Identity Manager, 11.1.2.3.0, 12.2.1.3.0 bertsioak
- Oracle iLearning, 6.1, 6.2 bertsioak
- Oracle Insurance Calculation Engine, 10.1.1, 10.2.1 bertsioak
- Oracle Insurance Rules Palette, 10.0, 10.1, 10.2, 11.0, 11.1 bertsioak
- Oracle Java SE, 6u201, 7u191, 8u182, 11 bertsioak
- Oracle Java SE Embedded, 8u18, 8u181 bertsioak
- Oracle JRockit, R28.3.19 bertsioa
- Oracle Outside In Technology, 8.5.3 bertsioa
- Oracle Real-Time Decision Server, 3.2.1 bertsioa
- Oracle Retail Allocation, 15.0, 16.0 bertsioak
- Oracle Retail Assortment Planning, 14.1, 15.0, 16.0 bertsioak
- Oracle Retail Back Office, 13.3, 13.4, 14, 14.1 bertsioak
- Oracle Retail Central Office, 14.1 bertsioa
- Oracle Retail Customer Management and Segmentation Foundation, 16.0, 17.0 bertsioak
- Oracle Retail Extract Transform and Load, 13.0, 13.1, 13.2 bertsioak
- Oracle Retail Financial Integration, 13.2, 14.0, 14.1, 15.0, 16.0 bertsioak
- Oracle Retail Integration Bus, 14.1.2 bertsioa
- Oracle Retail Invoice Matching, 15.0, 16.0 bertsioak
- Oracle Retail Open Commerce Platform, 5.3, 6.0, 6.0.1 bertsioak
- Oracle Retail Order Broker, 5.0, 5.1, 5.2, 15.0, 16.0 bertsioak
- Oracle Retail Point-of-Service, 13.4, 14.0, 14.1 bertsioak
- Oracle Retail Predictive Application Server, 14.0, 14.1, 15.0, 16.0 bertsioak
- Oracle Retail Returns Management, 14.1 bertsioak
- Oracle Retail Sales Audit, 15.0, 16.0 bertsioak
- Oracle Retail Xstore Point of Service, 6.5.12, 7.0.7, 7.1.7, 15.0.2, 16.0.4, 17.0.2 bertsioak
- Oracle Service Bus, 12.1.3.0.0, 12.2.1.3.0 bertsioak
- Oracle Transportation Management, 6.3.7 bertsioa
- Oracle Tuxedo, 12.1.1.0 bertsioa
- Oracle Virtual Directory, 11.1.1.7.0, 11.1.1.9.0 bertsioak
- Oracle VM VirtualBox, prior to 5.2.20 bertsioak
- Oracle WebCenter Portal, 11.1.1.9.0, 12.2.1.3.0 bertsioak
- Oracle WebCenter Sites, 11.1.1.8.0, 12.2.1.3.0 bertsioak
- Oracle WebLogic Server, 10.3.6.0, 12.1.3.0, 12.2.1.3 bertsioak, Docker 12.2.1.3.20180913 baino lehenagokoak
- OSS Support Tools, 18.4 baino lehenagoko bertsioak
- PeopleSoft Enterprise Interaction Hub, 9.1.0.0 bertsioa
- PeopleSoft Enterprise PeopleTools, 8.55, 8.56, 8.57 bertsioak
- Primavera Gateway, 15.2, 16.2, 17.12 bertsioak
- Primavera P6 Enterprise Project Portfolio Management, 8.4, 15.1, 15.2, 16.1, 16.2, 18.8, 17.7 - 17.12 bertsioak
- Primavera Unifier, 15.1, 15.2, 16.1, 16.2, 17.1-17.12, 18.1-18.8 bertsioak
- Siebel Applications, 18.7, 18.8, 18.9 bertsioak
- Solaris, 10, 11.3, 11.4 bertsioak
- SPARC Enterprise M3000, M4000, M5000, M8000, M9000 Servers, XCP 1123 bertsioa baino lehenagokoak
- Spatial, 2.0, 2.1, 2.2 bertsioak

**Azalpena:**

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

**Konponbidea:**

Eguneraketa horrek 301 ahultasun konpontzen ditu guztira, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna Erreferentzien atalean dagoen Oracleren loturan kontsulta daiteke.

**Xehetasuna:**

Kaltetutako produktuen araberako partxeak aplikatzea. Eguneraketak deskargatzeko informazioa Oraclek argitaratutako segurtasun buletinean lor daiteke.

**Etiketak:** Eguneraketa, Oracle, Ahultasuna

---

# Mugez kanpoko irakurketa erako ahultasuna

# VMware-n

**Argitalpen data:** 2018/10/17

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- VMware vSphere ESXi (ESXi), 6.7, 6.5 eta 6.0 bertsioak ESXi plataforman.
- VMware Workstation Pro / Player (Workstation), 14.x bertsioak edozein plataformatan.
- VMware Fusion Pro, Fusion (Fusion), 10.x bertsioak OS X plataforman.

**Azalpena:**

Anonymousek eta Trend Micro's Zero Day Initiativek larritasun kritikoko ahultasun baten berri eman diote VMwareri. Hori baliatuz erasotzaile batek mugez kanpoko irakurketa egin lezake.

**Konponbidea:**

Kaltetutako produktuetan ahultasuna konpontzeko, VMwarek ondoko partxeak argitaratu ditu:

- ESXi 6.7, 6.5 eta 6.0.
- Workstation Pro 14.1.3.
- Workstation Player 14.1.3.
- Fusion Pro / Fusion 10.1.3.

**Xehetasuna:**

VMware ESXi, Workstation eta Fusion-ek mugez kanpoko irakurketa erako ahultasuna daukate SVGA gailuetan, eta hori baliatuz erabiltzaile gonbidatu batek kodea exekuta lezake host-ean. Ahultasun horretarako CVE-2018-6974 identifikatzailea erabili da.

**Etiketak:** Eguneraketa, VMware, Ahultasuna

---

# Autentifikazioa saihestea libssh liburutegian

**Argitalpen data:** 2018/10/17

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- 0.8.4 eta 0.7.6 baino lehenagoko *libssh* bertsioak

**Azalpena:**

NCC Group-eko Peter Winter-Smith ikertzaileak ahultasun bat aurkitu du *libssh* liburutegian. Hori baliatuz, erasotzaile bat liburutegiaren kaltetutako bertsioak erabiltzen dituzten SSH saioetan kredentzialak sartu gabe autentifikatu liteke.

**Konponbidea:**

*libssh* 0.8.4 edo 0.7.6 bertsioetara eguneratzea.

**Xehetasuna:**

*SSH2_MSG_USERAUTH_SUCCESS* mezua zerbitzariari aurkez lekioke *SSH2_MSG_USERAUTH_REQUEST* mezuaren ordez, eta horrela autentifikazio prozesua saihets liteke. Ahultasun horretarako CVE-2018-10933 identifikatzailea erreserbatu da.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Hainbat ahultasun F5en BIG-IPn

**Argitalpen data:** 2018/10/18

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator):
  - 13.0.0tik 13.1.1era bitarteko bertsioak.
  - 12.1.0tik 12.1.3ra bitarteko bertsioak.
- BIG-IP APM Clients: 7.1.5etik 7.1.6ra bitarteko bertsioak.
- BIG-IP Edge Client: 7101etik 7160ra bitarteko bertsioak.

**Azalpena:**

Kritikotasun altu eta ertaineko hainbat ahultasun aurkitu dira BIG-IP plataformako produktuen hainbat modulutan. Ahultasun horiek baliatuz erasotzaile batek Cross-Site Scripting (XSS) bat exekuta lezake, politiken zerbitzarian *endpoints*-en egiaztapenak saihestuz fitxategi bat injekta lezake, edo erabiltzaileen beste konexio batzuetako saioetako datuak agerian utz litzake.

**Konponbidea:**

F5ek erabiltzaileen eskura jarri ditu ahultasunak konpontzeko hainbat eguneraketa, bertsioen arabera:

- 14.x adarreko bertsioetarako, 14.0.0.0 bertsiora eguneratzea.
- 13.x adarreko bertsioetarako, 13.1.1.2 bertsiora eguneratzea.
- 12.x adarreko bertsioetarako, 12.1.3.7 bertsiora eguneratzea.
- 7.1.x adarreko bertsioetarako, 7.1.7 bertsiora eguneratzea.

- 71xx adarreko bertsioetarako, 7170 bertsiora eguneratzea.

**Xehetasuna:**

Aurkitutako ahultasunak honakoak dira:

- BIG-IP Configuration utilitatearen erakutsi gabeko orri batean dagoen Cross-Site Scripting (XSS) erako ahultasun bat baliatuz, erabiltzaile autentifikatu batek JavaScript exekuta lezake une honetan konektatuta dagoen erabiltzailearentzat. Ahultasun hori baliatzeko, xede den host zehatzaren izena barnean hartzen duen eta bereziki diseinatuta dagoen URL bat bisitatu behar du erabiltzaileak. Ahultasun horretarako CVE-2018-15312 identifikatzailea erreserbatu da.
- APM Edge Client-ek duen ahultasun bat baliatuz, erasotzaile batek liburutegiko fitxategi bat injekta lezake, politiken zerbitzariak kargatuko duena, endpoints-en egiaztapenak saihestuz. Mac OS X eta Linux plataformetarako *endpoints*-en ikuskaritza osagaiak arazo hau pairatzen du. Ahultasun horretarako CVE-2018-15316 identifikatzailea erreserbatu da.
- Erasotzaile lokal batek XSS eraso bat egin lezake beste erabiltzaile batzuen sarbideak dituzten BIG-IP konfigurazio utilitatearen orrialdeetan islatuko litzatekeena. Ahultasun horretarako CVE-2018-15315 identifikatzailea erreserbatu da.
- Ahultasun hori gertatzeko ondoko baldintzak eman behar dira: APM BIG-IP sistema backend zerbitzariei NTLM SSO autentifikazioa egiteko konfiguratuta egotea eta, gainera, BIG-IP APM sistemaren aurrean proxy batek erabiltzaile ezberdinen konexioak multiplexatzea.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Hainbat ahultasun Drupal-en nukleoan

**Argitalpen data:** 2018/10/18

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Drupal, 7.x eta 8.x bertsioak

**Azalpena:**

Drupalek argitaratu duen segurtasun buletin batean 5 ahultasunen berri eman du. Horien ondorioz sarbide berezi batzuetarako baimenen saihestea, gune arbitrarioetara birbideratzeak edo urrunetik kodea exekutatzea gerta liteke.

**Konponbidea:**

Ezarrita dagoen bertsioaren arabera, ondoko bertsio hauetako batera eguneratu beharra dago: 7.60, 8.6.2 edo 8.5.8.

**Xehetasuna:**

Ondoren zehazten dira NISTen CMSSen arabera Drupalek Critical modura sailkatu dituen ahultasunak:

- Injekzioa *DefaultMailSystem::mail()*-en. Email bat bidaltzen denean, aldagai batzuk ez dira modu egokian garbitzen. Zehazki esateko, komandoen lerroan erabilitako argumentuak eduki litzakete. Egoera horren ondorioz, erasotzaile batek kodea exekuta lezake urrunetik.
- Testuinguruko loturen balioztapena. Lotura horien moduluak ez ditu modu nahikoan balioztatzen eskatutakoak. Ahultasun hau baliatu ahal izateko, erasotzaileak *access contextual links* baimena duen rol bat izan behar du, eta horren ondorioz urrunetik kodea exekuta liteke.

**Etiketak:** Eguneraketa, Edukien kudeatzailea, Ahultasuna

---

# Ahultasuna IBM Security Access Manager Appliance-n

**Argitalpen data:** 2018/10/18

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- IBM Security Access Manager Appliance, 9.0.3.1, 9.0.4.0 eta 9.0.5.0 bertsioak

**Azalpena:**

IBMk argitaratu duenez, ahultasun batek bere IBM Security Access Manager gailuei eragiten die, eta baimendu gabeko eragiketak egitea ahalbidetu lezake.

**Konponbidea:**

- 9.0.5.0 baino lehenagoko bertsioen kasuan, 9.0.5-ISS-ISAM-FP0000 bertsiora eguneratu.
- Eguneratu ondoren, 9.0.5.0 Interim Fix 2 aplikatu.

**Xehetasuna:**

- Segurtasun mailako ahultasun baten ondorioz, baimendu gabeko eragiketak gerta litezke Advanced Access Control zerbitzuak exekutatzen direnean. Ahultasun horretarako CVE-2018-1850 identifikatzailea erreserbatu da.

**Etiketak:** Eguneraketa, IBM, Ahultasuna

---

# Hainbat ahultasun Cisco produktuetan

**Argitalpen data:** 2018/10/18

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Cisco FXOS edo NX-OS softwarearen bertsio ahul bat exekutatzen duten eta LLDP protokoloa gaituta duten Cisco produktuak:
  - Firepower 4100 Series Next-Generation Firewall, 2.3 eta lehenagoko bertsioak.
  - Firepower 9300 Security Appliance.
  - MDS 9000 Series Multilayer Switches, 6.2 eta 5.2 bertsioak.
  - Nexus 2000 Series Switches, 6.0, 5.1 eta 5.0 bertsioak.
  - Nexus 3000 Series Switches, 6.0 (2) , 5.0 (3) eta 7.0 (3) I7 (3) bertsioak.
  - Nexus 3500 Platform Switches, 6.0 (2) eta 5.0 (3) bertsioak.
  - Nexus 5500, 5600 eta 6000 Platform Switches, 6.0, 5.1 eta 5.0 bertsioak.
  - Nexus 7000 eta 77000 Series Switches, 6.1 eta 5.2 bertsioak.
  - Nexus 9000 Series Fabric Switches, Aplikazioan Zentratutako Azpiegitura (ACI) moduan, 13.2 / 3.2 eta lehenagoko bertsioak.
  - Unified Computing System (UCS) 6100, 6200 eta 6300 Series Fabric Interconnects, 4.0, 3.2, 3.1, 2.2 eta lehenagoko bertsioak.
- Cisco NX-OS softwarearen bertsio ahul bat exekutatzen duten Cisco produktuak:
  - Cisco Nexus 5500, 5600 eta 6000 Series Switches, 7.3 eta lehenagoko bertsioak.
  - Nexus 3600 Platform Switches, 7.0 (3) F3 (4) bertsioak.
  - Nexus 9000 Series Switches, 7.0 (3) I7 (3) bertsioa modu independentean.
  - Nexus 9500 R-Series Line Cards and Fabric Modules, 7.0 (3) F3 (4) bertsioa.
- Cisco WLC, 8.7, 8.6, 8.5, 8.4, 8.3, 8.2, 8.1, 8.0 eta lehenagoko bertsioak.
- Cisco sarbide puntuak, 8.5 bertsioa eta lehenagokoak dituztenak.

**Azalpena:**

Ciscok bere hainbat produkturi buruzko 7 ahultasun argitaratu ditu, denak larritasun altukoak.

**Konponbidea:**

Ciscok erabiltzaileen eskura jarri ditu hainbat eguneraketa, kaltetutako produktuaren arabera.

- Cisco Softwarearen deskarga panela.

**Xehetasuna:**

Ahultasun horietako batzuk arrakastaz baliatuz gero, ondokoak eragin litezke:

- Zerbitzua ukatzea (DoS).
- Pribilegioen eskalatzea.
- Informazioa ezagutaraztea.

Ahultasun horietarako ondoko identifikatzaileak esleitu dira: CVE-2018-0417, CVE-2018-0441, CVE-2018-0442, CVE-2018-0443, CVE-2018-0456, CVE-2018-0378 eta CVE-2018-0395.

**Etiketak:** Eguneraketa, Cisco, Komunikazioak, Ahultasuna

---

# Ahultasuna Cisco Webex Meetings Desktop App Update Service-n

**Argitalpen data:** 2018/10/25

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Cisco WebEx Meetings Desktop App, 33.6.0 bertsioaren aurrekoak.
- Cisco Webex Productivity Tools, 32.6.0 eta ondoreneko bertsioak, 33.0.5 bitartean

**Azalpena:**

Windowserako Cisco Webex Meetings Desktop App-ek eguneratze zerbitzuan duen ahultasun bat baliatuz, erasotzaile lokal autentifikatu batek komando arbitrarioak exekuta litzake erabiltzaile pribilegiatu baten modura.

**Konponbidea:**

Cisco Webex Meetings Desktop App eta Cisco Webex Productivity Tools eguneratzea.

**Xehetasuna:**

Erabiltzaileak ematen dituen parametroen baliozkotze ez aski baten erako ahultasun bat baliatuz, erasotzaile batek *update service* komandoa dei lezake bereziki diseinatutako argumentu baten bidez, eta komando arbitrarioak exekutatzea lor lezake SYSTEM erabiltzaile baten baimenekin.

**Etiketak:** Eguneraketa, Cisco, Ahultasuna

---

# Sandbox ihesa Jenkins-en hainbat pluginetan

**Argitaratze-data:** 2018/10/30

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Pipeline: Groovy Plugin
- Script Security Plugin

**Azalpena:**

Segurtasun abisu bat argitaratu da; erasotzaile batek ihes egin liezaieke, Groovy Sandbox liburu-dendak emandako babes mekanismoei.

**Konponbidea:**

Pluginak honako bertsioetara eguneratzea:

- Pipeline: Groovy Plugin 2.60
- Script Security Plugin 1.48

**Xehetasuna:**

Script Security Plugin eta Pipeline Groovy Pluginek erabilitako Groovy Sandbox liburutegiak ez ditu muga jakin batzuk aplikatzen metodoak bukatzeko. Eraikitzaile eta metodo arbitrarioak deitzeko erabil liteke, sandbox delakoaren babesa saihestuz.

**Etiketak:** Eguneraketa, Ahultasuna

---

# Hainbat ahultasun F5 produktu batzuetan

**Argitaratze-data:** 2018/10/31

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, PSM, GTM, Link Controller, PEM, WebAccelerator, Websafe): *Erreferentzien* atala kontsultatzea, kaltetutako bertsio zehatzak errebisatzeko.Enterprise Manager: 3.1.1 bertsioa.
- BIG-IQ Centralized Management:
  - 6.0.0tik 6.0.1era bitarteko bertsioak.
  - 5.0.0tik 5.4.0era bitarteko bertsioak.
  - 4.6.0 bertsioa.
- BIG-IQ Cloud eta Orchestration: 1.0.0 bertsioa.
- F5 iWorkflow: 2.0.1tik 2.3.0era bitarteko bertsioak.

**Azalpena:**

Kritikotasun handi, ertain eta baxuko hainbat ahultasun antzeman dira hainbat produktutan, hala nola BIG-IP, Enterprise Manager, BIG-IQ Centralized Management, BIG-IQ Cloud eta Orchestration eta F5 iWorkflow. Ahultasun horien ondorioz, gailuen konfigurazioan akats bat egon liteke, TMM (*Traffic Management Microkernel*) delakoaren berrabiarazte batengatik, zerbitzu ukapenaren inguruko erasoengatik, trafikoa eteteagatik, egiaztatutako erabiltzaileentzako pribilegioak baliatzeagatik, sistemako artxibo kritikoak berridazteagatik, memoria faltagatik eta sisteman sarbidea izan dezaketen ziurtagiri ezeztatuak dituzten erabiltzaileengatik.

**Konponbidea:**

F5 etxeak hainbat eguneraketa jarri ditu erabiltzaileen esku, ahultasun horiek konpontzeko. Partxeak software deskarga zentroan ere aurki daitezke.

**Xehetasuna:**

Kritikotasun handiko ahultasunak honakoak dira:

- BIG-IP sistemak aldi baterako akats bat sortzen du trafikoa prozesatzeko unean, *Traffic Management Microkernel (TMM)* berrabiarazte baten ostean, eta talde batean konfiguratutako gailuek huts egin dezakete. Ahultasun horretarako, CVE-2018-15318 identifikatzailea erreserbatu da.
- Ahultasun horren ondorioz, urrutiko erasotzaileek zerbitzu ukapen bat izan dezakete BIG-IP sisteman. Ahultasun horretarako, CVE-2018-15317 identifikatzailea erreserbatu da.
- Errebelatu gabeko trafiko patroiek zerbitzu ukapen bidezko eraso bat eragin dezakete, BIG-IP sistemarako. Ahultasun hori agerian uzten duen konfigurazioa BIG-IP sistemaren beraren IPa da; VLAN taldekoa eta portuen blokeoa konfiguratuta daukana, *allow-all* ez den beste edozerekin. Ahultasun horretarako, CVE-2018-15320 identifikatzailea erreserbatu da.
- Erasotzaile batek trafikoa eten lezake edo BIG-IP sistemaren hutsegitea eragin, taldeko beste gailu bati eraginez. Ahultasun horretarako, CVE-2018-15320 identifikatzailea erreserbatu da.

Kritikotasun ertain edo baxuko gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2018-15327, CVE-2018-15324, CVE-2018-15323, CVE-2018-15322, CVE-2018-15321, CVE-2018-15325 eta CVE-2018-15326.

**Etiketak:** Eguneraketa, Ahultasuna