
# 2018ko Apirilaren Bulletina

## Ohartarazpenak - Teknikoak

---

## Hainbat ahultasun Ciscoren IOS eta IOS XE sistemetan

**Argitaratze-data:** 2018/04/02

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Cisco IOS.
- Cisco IOS XE.

**Azalpena:**

Hainbat ahultasun kritiko antzeman dira IOS edo IOS XE erabiltzen duten Cisco gailuetan. Ahultasun horien ondorioz, egiaztatu gabeko urrutiko erasotzaile batek zerbitzu ukapena eragin dezake edo kodearen exekuzio arbitrarioa, pribilegioen igoerarekin.

Kritikotasun handiko hainbat ahultasun antzeman dira produktu horietan. Informazio gehiago, Ciscoren web orri ofizialean.

**Konponbidea:**

Ciscok ahultasun horiek konpontzeko doako eguneratze bat argitaratu du. Gailuak ahultasuna izan dezakeen ala ez jakiteko, Ciscok on line tresna bat argitaratu du.

- Cisco IOS Software Checker.

Zerbitzu-kontraturen bat indarrean duten erabiltzaileek eguneraketa bat deskargatu dezakete produktuaren ahultasuna konpontzeko, honako helbidean:

- https://software.cisco.com/download/navigator.html

Ez baduzu zerbitzu-kontraturik, mesedez, kontsultatu Cisco TAC zerbitzuarekin:

- https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

**Xehetasuna:**

Kritikotasun handiko ahultasunak honakoak dira:

- Cisco IOS eta IOS Xeren Smart Installeko ahultasun batek, gailuaren TCP 4786 portura gaizki osatutako pakete bat bidaltzean egindako okerreko balioztatze baten ondoriozkoa, egiaztatu gabeko urrutiko erasotzaile bati aukera eman ahal dio zerbitzu ukapen egoera bat sortzeko edo kodearen exekuzio arbitrariorako. Ahultasun horretarako, CVE-2018-0171 identifikatzailea erreserbatu da.
- Cisco IOSeko ahultasun batek egiaztatu gabeko erasotzaile bat aukera eman ahal dio kaltetutako gailura sartzeko, gailuaren lehendabiziko abiaraztean erabiltzen den erabiltzaile eta pasahitzarekin. Ahultasun horren ondorioz, gailura sartzeko aukera egon liteke, 15 mailako pribilegioak dituen kontu batekin. CVE-2018-0150 identifikatzailea erreserbatu da ahultasun horretarako.
- Cisco IOS eta IOS XE gailuen Quality of Service (QoS) azpisistemako ahultasun batek, 18999 portura bideratutako UDP pakete batzuen mugen konprobaketa oker baten ondoriozkoak, aukera eman liezaioke urrutiko erasotzaile bati bufferraren gainezkatzea eragiteko, zerbitzuaren ukapen egoera edo kodearen exekuzio arbitrarioa sortuz, pribilegioen igoerarekin.

**Etiketak:** Eguneratzea, Cisco, Ahultasuna

---

## Intel SPI oinarri duten produktuetako eragiketa-kode ez seguruak

**Argitaratze-data:** 2018/04/04

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- Intel® CoreTM markako prozesagailuen 5., 6., 7. eta 8. belaunaldiak.
- Intel® Pentium® eta Celeron® N3520, N2920 y N28XX prozesagailuak
- Intel® AtomTM x7-Z8XXX, x5-8XXX prozesagailu-familia.
- Intel® PentiumTM J3710, N37XX, J4205 eta N4200 prozesagailuak.
- Intel® CeleronTM J3XXX prozesagailuak.
- Intel® AtomTM x5-E8000 eta x7-E39XX prozesagailuak.
- Intel® Celeron® J3455, J3355, N3350, eta N3450 prozesagailuak.
- Intel® Xeon® Scalable prozesagailuak.
- Intel® Xeon® E3 v6, E3 v5, E7 v4, E7 v3 eta E7 v2 prozesagailuak.
- Intel® Xeon® PhiTM x200 prozesagailuak.
- Intel® Xeon® D prozesagailu- familia.
- Intel® AtomTM C prozesagailu-seriea.

**Azalpena:**

Intelek larritasun handiko ahultasun bat argitaratu du. Horren ondorioz, erasotzaile batek zerbitzu ukapen bat ekar lezake kaltetutako produktuetan.

**Konponbidea:**

Intelek gomendatzen du kaltetutako sistemen fabrikatzaileen laguntza eremuak egiaztatzea, azken segurtasun-eguneraketak instalatuta daudela konprobatzeko.

Eguneraketa partxeen inguruko informazio eta deskargarako: http://www.intel.com/support/

**Xehetasuna:**

SPI Flash delakoaren konfigurazioaren ondorioz, tokiko erasotzaile batek jokabidea aldatu eta zerbitzu ukapen bat eragin lezake. Ahultasun horretarako, CVE-2017-5703 identifikatzailea erreserbatu da.

**Etiketak:** Ahultasuna

---

# Microsoft Malware Protection Engine ahultasun handia

**Argitaratze-data:** 2018/04/05

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Forefront Endpoint Protection 2010
- Microsoft Security Essentials
- Windows Defender
- Windows Intune Endpoint Protection

**Azalpena:**

Microsoftek segurtasun partxe bat argitaratu du ziklotik kanpo, Microsoft Malware Protection Engine delakorako.

**Konponbidea:**

Kaltetutako sistema eguneratzea, Microsoftek banatutako partxe automatikoen bidez.

**Xehetasuna:**

Microsoften malwarearen aurkako motorrak memoriaren korrupzioaren ahultasun bat dauka, eta kodearen exekuziorako aukera ematen du, SYSTEM pribilegioekin, manipulatutako artxibo bat eskaneatzen denean malware bila. Azterketa hori automatikoki egiten da, denbora errealeko babesa aktibatuta dagoenean. Ahultasun horretarako CVE-2018-0986 kodea erreserbatu da.

**Etiketak:** Microsoft, Ahultasuna

---

# IBMren SPSS Statistics tresnari eragiten dioten ustezko ahultasunak GSKit softwarean

**Argitaratze-data:** 2018/04/06

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- IBM SPSS Statistics-en honako bertsioak.
  - 21.0.0.2
  - 22.0.0.2
  - 23.0.0.3
  - 24.0.0.2
  - 25.0.0.1

**Azalpena:**

Hainbat ahultasun antzeman dira, horietako bat kritikotasun altukoa. Egiaztatu gabeko urruneko erasotzaile batek informazio handia sortu dezake kaltetutako produktuetatik.

**Konponbidea:**

IBMk eguneratze batzuk argitaratu ditu, ahultasun horiek konpontzeko. Eguneratzeak kaltetutako produktuaren bertsioaren araberakoak dira:

- SPSS Statistics 21.0.0.2: Statistics 21 FP002 IF016
- SPSS Statistics 22.0.0.2: Statistics 22 FP002 IF017
- SPSS Statistics 23.0.0.3: Statistics 23 FP003 IF013
- SPSS Statistics 24.0.0.2: Statistics 24 FP002 IF010
- SPSS Statistics 25.0.01: Statistics 25 FP001 IF006

Eguneratze horiek egiteko, IBMko erabiltzaile kontua eduki beharra dago.

**Xehetasuna:**

Kritikotasun handiko ahultasun horren ondorioz, erasotzaile batek IBMren GSKit konprometitu lezake eta PRNG egoera bikoiztu liteke sistema deien bidez (fork), hainbat ICC instantzia kargatzen direnean. Horrek eragin lezake bikoiztutako ID saioak sortzea eta funtsezko materiala bikoiztea. Ahultasun horretarako, CVE-2018-1426 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, IBM, Ahultasuna

---

# 2018ko apirileko Microsoften segurtasun-buletinak

**Argitaratze-data:** 2018/04/11

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office and Microsoft Office Services and Web Apps
- ChakraCore
- Adobe Flash Player
- Microsoft Malware Protection Engine
- Microsoft Visual Studio
- Microsoft Azure IoT SDK

**Azalpena:**

Segurtasun eguneraketen inguruko hileroko Microsoft argitalpenean 66 ahultasun jaso dira oraingoan; 22 kritiko gisa sailkatu dira eta 44 garrantzitsu gisa. Gainerakoak larritasun baxu edo ertainekoak dira.

**Konponbidea:**

Dagokion eguneraketa instalatzea. Instalazioari buruzko informazio orrian eguneratzeko metodoen inguruko informazioa jaso da:

**Xehetasuna:**

Otsaileko segurtasun eguneraketen buletinean mota hauetako hainbat segurtasun-ahultasun argitaratu dira:

- Zerbitzua ukatzea.
- Pribilejioen eskalatzea.
- Informazioa zabaltzea.
- Kodearen urrutiko exekuzioa.
- Segurtasunari ihes egitea.

**Etiketak:** Eguneratzea, Microsoft, Nabigatzailea, Pribatutasuna, Sistema Eragilea, Ahultasuna

---

# 2018ko apirileko SAP segurtasunaren eguneratzea

**Argitaratze-data:** 2018/04/11

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- SAP Business Client
- SAP Business One
- SAP Visual Composer
- SAP Business Objects
- SAP Cloud Platform Connector
- SAP Disclosure Management
- SAP Solution Manager
- Sybase PowerBuilder
- SMP
- Agentry
- SAP Open Switch
- SAP Open Server
- SDK for SAP ASE
- SYBASE SOFTWARE DEV KIT

- SYBASE IQ
- SAP IQ
- Sybase SQL Anywhere
- SAP SQL Anywhere
- SAP SQL Anywhere OnDemand
- SAP ASE
- SAP Replication Server
- SYBASE ECDA
- SAP HANA Smart Data Streaming
- SAP Complex Assembly Manufacturing
- SAP Data Services
- SAP Crystal Reports Server, OEM Edition
- SAP Control Center and SAP Cockpit Framework

**Azalpena:**

SAPek produktu batzuen inguruan hainbat segurtasun eguneraketa argitaratu ditu, bere hileroko jakinarazpenean.

**Konponbidea:**

SAPen laguntzarako ataria bisitatu eta eguneratze edo partxeak instalatzea, fabrikatzaileak adierazitakoaren arabera.

**Xehetasuna:**

SAPek 8 segurtasun ohar eta 4 eguneraketa egin ditu bere hileroko jakinarazpenean. Horietako batek larritasun kritikoa dauka eta gainerakoek tartekoa.

Argitaratutako ahultasun mota honakoei dagokie:

- Kodearen injekzioaren 2 ahultasun.
- Cross-site scripting delakoaren 2 ahultasun.
- Informazioaren dibulgazioaren arloko 2 ahultasun.
- Zerbitzu ukapenaren inguruko ahultasun bat.
- Direktorio ibilbideen okerreko mugaketaren ahultasun bat (Directory/Path transversal).
- Beste motaren bateko 4 ahultasun.

Kritikotzat jotako segurtasun oharra honakoei dagokio:

- Memoriaren korrupzioa: Erasotzaile batek berariaz diseinatutako memoria kode bat injektatu lezake, eta horrek zerbitzuaren ukapena edo kodearen urrutiko exekuzioa eragin litzake.

Larritasun handiko gisa etiketatuta daudenei dagokienez, horietako bat zerbitzu-ukapen bat da, beste bat SAP Business Objects-eko saioen okerreko erabilera bat eta beste bi aurreko segurtasun oharren eguneratzeak.

**Etiketak:** Eguneratzea, SAP, Ahultasuna

---

# Hainbat ahultasun Juniper produktuetan

**Argitaratze-data:** 2018/04/12

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Junos OS bertsio hauek:
  - 13.2.
  - 14.1X53.
  - 15.1.
  - 15.1X49.
  - 15.1X53.
  - 16.1.
  - 16.2.
  - 17.1.
  - 17.2.
  - 17.2X75.
- Junos OS SRX Serie bertsio hauek:
  - 12.1X46.
  - 12.3X48.
  - 15.1X49.Steel-Belted Radius Carrier:
    - 8.4.1 8.4.1-R5en aurreko bertsioak.
    - 8.3.0 8.3.0-R11ren aurreko bertsioak.
    - 8.2.0 8.2.0-R18ren aurreko bertsioak.
- NSM Appilance:
  - Network and Security Manager Appliance 2012.2
- Junos OS VPLS konfiguratuta eta exekuzioan:
  - 12.1X46.
  - 12.3X48.
  - 14.1.
  - 14.1X53.
  - 14.2.
  - 15.1.
  - 15.1X49.
  - 15.1X53.
  - 16.1.
  - 16.2.
  - 17.1.
  - 17.2.

**Azalpena:**

Hainbat ahultasun antzeman dira honakoetan: Juniper OS, Juniper OS SRXean, Juniper OS VPLSrekin (konfiguratuta eta exekuzioan) eta

NSM Appilance. Larritasun kritikoko 2 ahultasun eta larritasun handiko 13 ahultasun daude. Ahultasun horiek eragin lezakete urrutiko erasotzaile batek honakoak burutzea:

- Kodearen exekuzio arbitrarioa.
- Sistema berrabiaraztea.
- Pasahitzak ezagutaraztea.
- Pribilegioak igotzea.
- Zerbitzuen ukapenerako baldintza bat sortzea.
- Informazioa filtratzea.

**Konponbidea:**

Juniperrek erabiltzaileen esku jarri ditu hainbat partxe, ahultasunak konpontzeko, betiere kaltetutako produktuaren arabera. Partxe horiek orri honetan deskargatu daitezke: Juniperren laguntza orria

Laguntza eremura sartzeko, Juniperren erabiltzaile kontu bat izan behar duzu.

**Xehetasuna:**

Larritasun kritikoa duten ahultasunak honakoak dira:

- Junos OS delakoan, urrutiko erasotzaile batek datagrama bat sor lezake Connectionless Network Protocol (CLNP) delakorako, berariaz sortua, gailuaren Junos OS interfaze espezifikorako. Horrek kernel delakoa ezustean itxi eta kodearen urrituko exekuzioa baimendu lezake. Ahultasun horretarako, CVE-2018-0016 identifikatzailea erreserbatu da.
- Junos OS delakoan, egiaztatu gabeko urrutiko erasotzaile batek kodearen exekuzio bat egin lezake, PHP bertsio zaharretan aurretik askatutako memoriaren erabileraren akats baten ondorioz, URL PHP bidez manipulatutako datuen injekzioaren bidez, J-Web prozesuaren testuinguruko espezifikoak. Ahultasun horretarako, CVE-2018-0001 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, Sistema Eragilea, Ahultasuna

---

# Hainbat ahultasun F5 produktu batzuetan

**Argitaratze-data:** 2018/04/13

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- BIG-IP (Analytics, LTM, AAM, AFM, APM, ASM, DNS, Edge, Gateway, GTM Link Controller, PEM, WebAccelerator, WebSafe) honako bertsioetan:
  - 11.5.4 HF4 - 11.5.5
- BIG-IP (LTM, AAM, AFM, APM, ASM, Link Controller, PEM, WebSafe) honako bertsioetan:
  - 13.0.0
  - 12.0.0 - 12.1.3
  - 11.6.1 - 11.6.2 eta 11.5.1 - 11.5.5

**Deskribapena:**

Larritasun handiko 2 ahultasun argitaratu dira. Horien bidez, erasotzaile batek zerbitzua ukatzeko hainbat baldintza eragin ditzake kaltetutako produktuetan.

**Konponbidea:**

Kaltetutako bertsioa eguneratzea, produktuaren adarraren arabera, honako baten batera:

- 13.1.0 o 13.0.1
- 12.1.3.2
- 11.6.3 o 11.5.6

**Xehetasuna:**

- Trafikoaren Kudeaketarako Microkernel delakoak (TMM) iraulketa artxibo bat sor lezake (core file) eta berrabiarazi, IPv6 zerbitzari birtualetan pakete sekuentzia espezifiko bat prozesatzean. Ahultasun horretarako CVE-2018-5510 identifikatzailea erreserbatu da.
- BIG-IP sistema baten bidez egindako proxy SOCKS eskaeren erantzunek Trafikoaren Kudeaketarako Microkernel (TMM) delakoak ematen duen zerbitzua eten lezakete. Datuen planoa eraginpean geratzen da soilik zerbitzari birtual bati proxy SOCKS profil bat gehitzen zaionean. Kontrol-planoari ez lioke eragingo ahultasun honek. Ahultasun horretarako, CVE-2018-6148 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, Ahultasuna

---

# Hainbat ahultasun VMware-ren vRealize Automation sisteman

**Argitaratze-data:** 2018/04/16

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- VMware vRealize Automation (vRA) bertsioak:
  - 7.3.x
  - 7.2.x
  - 7.1.x
  - 7.0.x

**Azalpena:**

ERNW Enno Rey Netzwerke GmbH-eko Oliver Matula eta Benjamin Schwendemann ikertzaileek bi ahultasun antzeman dituzte. Horren ondorioz, erasotzaile batek erabiltzaile baten ekipoa kolokan jarri edo erabiltzaile baten saioa bahitu lezake.

**Konponbidea:**

VMware erakundeak bi eguneraketa jarri ditu erabiltzaileen esku, ahultasun horiek konpontzeko. Honako loturen bidez deskargatu daitezke:

- 7.3.1 bertsioa
- 7.4.0 bertsioa

**Xehetasuna:**

Aurkitutako ahultasunak honakoak dira:

- DOM delakoan oinarritutako Cross-site scripting motako ahultasun baten ondorioz, erasotzaileak erabiltzailearen vRA ekipoa kolokan jar dezake.  Ahultasun horretarako CVE-2018-6958 identifikatzailea erreserbatu da.
- Tarteko larritasuna duen ahultasunerako CVE-2018-6959 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, VMware, Ahultasuna

---

# Eguneraketa kritikoak Oraclen (2018ko apirila)

**Argitaratze-data:** 2018/04/18

**Garrantzia:** kritikoa

**Kaltetutako baliabideak:**

- Enterprise Manager Base Platform, 12.1.0.5, 13.2.0.0 bertsioak
- Enterprise Manager for MySQL Database, 12.1.0.4 bertsioa
- Enterprise Manager for Virtualization, 13.2 bertsioa
- Enterprise Manager Ops Center, 12.2.2, 12.3.3 bertsioak
- Hardware Management Pack, 2.4.3aren aurreko bertsioak
- Instantis EnterpriseTrack, 17.1, 17.2 bertsioak
- Integrated Lights Out Manager (ILOM), 3.x, 4.x bertsioak
- JD Edwards EnterpriseOne Tools, 9.2.2 bertsioa
- JD Edwards World Security, A9.2, A9.3, A9.4 bertsioak
- Management Pack for Oracle GoldenGate, 11.2.1.0.13 bertsioa
- MICROS Handheld Terminal, Fusion 2.03.0.0.021Ren aurreko bertsioak
- MICROS Lucas, 2.9.5 bertsioa
- MySQL Cluster, 7.2.27 bertsioa eta aurrekoak, 7.3.16 eta aurrekoak, 7.4.14 eta aurrekoak, 7.5.5 eta aurrekoak.
- MySQL Enterprise Monitor, 3.3.7.3306 bertsioa eta aurrekoak, 3.4.5.4248 eta aurrekoak, 4.0.2.5168 eta aurrekoakMySQL Server, 5.5.59 bertsioa eta aurrekoak, 5.6.39 eta aurrekoak, 5.7.21 eta aurrekoak.Oracle Access Manager, 10.1.4.3.0, 11.1.2.3.0, 12.2.1.3.0 bertsioak
- Oracle Adaptive Access Manager, 11.1.2.3.0 bertsioa
- Oracle Agile Engineering Data Management, 6.1.3, 6.2.0, 6.2.1 bertsioak
- Oracle Agile PLM Framework, 9.3.6 bertsioa
- Oracle Agile Product Lifecycle Management for Process, 6.1.1.6, 6.2.0.0, 6.2.1.0 bertsioak
- Oracle Application Testing Suite, 12.5.0.3, 13.1.0.1, 13.2.0.1 bertsioak
- Oracle Banking Corporate Lending, 12.3.0, 12.4.0, 12.5.0, 14.0.0 bertsioak
- Oracle Banking Enterprise Collections, 2.6 bertsioa
- Oracle Banking Enterprise Originations, 2.6 bertsioa
- Oracle Banking Enterprise Product Manufacturing, 2.6 bertsioa
- Oracle Banking Payments, 12.3.0, 12.4.0, 12.5.0, 14.0.0 bertsioak
- Oracle Banking Platform, 2.4, 2.5, 2.6 bertsioak
- Oracle Big Data Discovery, 1.6.0 bertsioa
- Oracle Business Intelligence Data Warehouse Administration Console, 11.1.1.6.4 bertsioa
- Oracle Business Intelligence Enterprise Edition, 11.1.1.7.0, 11.1.1.9.0, 12.2.1.2.0, 12.2.1.3.0 bertsioak
- Oracle Communications Calendar Server, 8.x bertsioa
- Oracle Communications Calendar Server, 8.x bertsioaOracle Communications EAGLE LNP
- Application Processor, 10.1.0.0.0 bertsioak eta aurrekoak
- Oracle Communications Calendar Server, 8.x bertsioa
- Oracle Communications MetaSolv Solution, 6.3.0 bertsioa
- Oracle Communications Network Charging and Control, 4.4.1.5.0, 5.0.0.1.0, 5.0.0.2.0, 5.0.1.0.0, 5.0.2.0.0 bertsioak
- Oracle Communications Network Intelligence, 7.3.x bertsioa
- Oracle Communications Order and Service Management, 7.2.4.3.0, 7.3.0.1.x, 7.3.1.0.7, 7.3.5.0.x bertsioak
- Oracle Communications Unified Inventory Management, 7.x bertsioa
- Oracle Data Visualization Desktop, 12.2.4.1.1 bertsioa
- Oracle Database Server, 11.2.0.4, 12.1.0.2, 12.2.0.1, 18.1.0.0 bertsioak
- 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, 3.2 bertsioak
- Oracle Endeca Information Discovery Integrator, 7.6.1.0.0, 7.7.0.0.0 bertsioak
- Oracle Endeca Server, 7.7 bertsioa
- Oracle Enterprise Repository, 11.1.1.7.0, 12.1.3.0.0 bertsioak
- Oracle Financial Services Analytical Applications Infrastructure, 7.3.x, 8.0.x bertsioak
- Oracle Financial Services Basel Regulatory Capital Basic, 8.0.x bertsioa
- Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach, 8.0.x bertsioa
- Oracle Financial Services Hedge Management and IFRS Valuations, 8.0.4, 8.0.5 bertsioak
- Oracle Financial Services Market Risk Measurement and Management, 8.0.5 bertsioa
- Oracle FLEXCUBE Core Banking, 11.5.0, 11.6.0, 11.7.0 bertsioa
- Oracle FLEXCUBE Enterprise Limits and Collateral Management, 12.3.0, 14.0.0 bertsioak
- Oracle FLEXCUBE Investor Servicing, 12.0.4, 12.1.0, 12.3.0, 12.4.0 bertsioak
- Oracle FLEXCUBE Private Banking, 12.0.0, 12.1.0 bertsioak
- Oracle FLEXCUBE Universal Banking, 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 bertsioak
- Oracle Fusion Applications, 11.1.2 through 11.1.9 bertsioak
- Oracle Fusion Middleware, 11.1.1.7, 11.1.1.9, 11.1.2.3, 12.1.3.0, 12.2.1.2, 12.2.1.3 bertsioak
- Oracle Fusion Middleware MapViewer, 11.1.1.7.0, 11.1.1.9.0 bertsioak
- Oracle GoldenGate, 12.2.0.1 bertsioa
- Oracle GoldenGate Veridata, 11.2.0.1.2, 12.1.3.0.0 bertsioak

- Oracle Hospitality Cruise Fleet Management System, 9.x bertsioa
- Oracle Hospitality Guest Access, 4.2.0, 4.2.1 bertsioak
- Oracle Hospitality Reporting and Analytics, 9.0 bertsioa
- Oracle Hospitality Simphony, 2.7, 2.8, 2.9, 2.10 bertsioak
- Oracle Hospitality Simphony First Edition, 1.6, 1.7 bertsioak
- Oracle Hospitality Suite8, 8.x bertsioa
- Oracle HTTP Server, 12.1.3, 12.2.1.2 bertsioak
- Oracle Java SE, 6u181, 7u161, 7u171, 8u152, 8u162, 10 bertsioak
- Oracle Java SE Embedded, 8u152, 8u161 bertsioak
- Oracle JRockit, R28.3.17 bertsioa
- Oracle Managed File Transfer, 12.1.3.0.0, 12.2.1.2.0, 12.2.1.3.0 bertsioak
- Oracle Mobile Security Suite, 3.0.1 bertsioa
- Oracle Outside In Technology, 8.5.3 bertsioa
- Oracle Retail Advanced Inventory Planning, 13.2, 13.4, 14.1, 15.0 bertsioak
- Oracle Retail Back Office, 13.4.9, 14.0.4, 14.1.3 bertsioak
- Oracle Retail Central Office, 13.4.9, 14.0.4, 14.1.3 bertsioak
- Oracle Retail Customer Engagement, 16.0 bertsioa
- Oracle Retail EFTLink, 1.1.125, 15.0.2, 16.0.3 bertsioak
- Oracle Retail Insights, 14.0, 14.1, 15.0, 16.0 bertsioak
- Oracle Retail Integration Bus, 13.2 bertsioa
- Oracle Retail Invoice Matching, 12.0, 13.0, 13.1, 13.2, 14.0, 14.1, 15.0, 16.0 bertsioak
- Oracle Retail Merchandising System, 16.0 bertsioak
- Oracle Retail Order Broker, 5.0, 5.1, 5.2, 15.0, 16.0 bertsioak
- Oracle Retail Order Management System, 4.0, 4.5, 4.7, 5.0 bertsioak
- Oracle Retail Point-of-Service, 13.3.8, 13.4.9, 14.0.4, 14.1.3 bertsioak
- Oracle Retail Predictive Application Server, 13.4.3, 14.0.3, 14.1.3 bertsioak
- Oracle Retail Price Management, 12.0, 13.0, 13.1, 13.2, 14.0, 14.1, 15.0, 16.0 bertsioak
- Oracle Retail Returns Management, 2.3.8, 2.4.9, 14.0.4, 14.1.3 bertsioak
- Oracle Retail Store Inventory Management, 12.0.12, 13.0.7, 13.1.9, 13.2.9, 14.0.4, 14.1.3, 15.0.2, 16.0.1 bertsioak
- Oracle Retail Xstore Point of Service, 6.0, 6.0.12, 6.5, 6.5.12, 7.0, 7.0.7, 7.1, 7.1.7, 15.0, 15.0.2, 16.0, 16.0.3 bertsioak
- Oracle Secure Global Desktop (SGD), 5.3 bertsioa
- Oracle Security Service, 12.1.3.0.0, 12.2.1.2.0 bertsioak
- Oracle Transportation Management, 6.2, 6.4.3 bertsioak
- Oracle Tuxedo, 12.1.1.0.0 bertsioak
- Oracle Utilities Framework,  2.2.0, 4.2.0, 4.3.0 bertsioak
- Oracle VM VirtualBox, 5.1.36 aurreko bertsioak, 5.2.10 aurrekoa
- Oracle WebCenter Content, 11.1.1.9.0, 12.2.1.2.0, 12.2.1.3.0 bertsioak
- Oracle WebCenter Portal, 12.2.1.2.0, 12.2.1.3.0 bertsioak
- Oracle WebCenter Sites, 11.1.1.8.0, 12.2.1.2.0, 12.2.1.3.0 bertsioak
- Oracle WebLogic Portal, 10.3.6.0.0 bertsioa
- Oracle WebLogic Server, 10.3.6.0, 12.1.3.0, 12.2.1.2, 12.2.1.3 bertsioak
- OSS Support Tools, 18.2 aurreko bertsioak
- PeopleSoft Enterprise HCM, 9.2 bertsioa
- PeopleSoft Enterprise HCM Shared Components, 9.2 bertsioa
- PeopleSoft Enterprise PeopleTools, 8.54, 8.55, 8.56 bertsioak
- PeopleSoft Enterprise PRTL Interaction Hub, 9.1 bertsioa
- PeopleSoft Enterprise PT PeopleTools, 8.54, 8.55, 8.56 bertsioak
- Primavera P6 Enterprise Project Portfolio Management, 16.2, 17.1 ? 17.12 bertsioak
- Primavera Unifier, 16.x, 17.x bertsioak
- Real-Time Decisions (RTD) Solutions, 3.2.0.0.0 bertsioa
- Siebel Applications, 17.0 bertsioa
- Solaris, 10, 11.3 bertsioak
- Solaris Cluster, 4.3 bertsioa
- Sun ZFS Storage Appliance Kit (AK), 8.7.17 aurreko bertsioa

**Azalpena:**

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

**Konponbidea:**

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

**Xehetasuna:**

Eguneraketa horrek 254 ahultasun konpontzen ditu, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna Oracleren loturan dagoen Erreferentzien atalean kontsulta daiteke.

**Etiketak:** Eguneraketa, Oracle

---

# Hainbat ahultasun Cisco produktuetan

**Argitaratze-data:** 2018/04/19

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

- Cisco WebEx Business Suite (WBS31) client builds, T31.23.2 bertsioaren aurrekoak.
- Cisco WebEx Business Suite (WBS32) client builds, T32.10 bertsioaren aurrekoak.
- Cisco WebEx Meetings client builds, T32.10 bertsioaren aurrekoak.
- Cisco WebEx Meetings Server builds, 2.8 MR2 bertsioaren aurrekoak.
- Cisco Unified Computing System (UCS) Director 6.0 eta 6.5 bertsioak, berez datorren konfigurazioan dagoen patch 3 baino lehenagokoak.
- Aggregation Services Router (ASR) 5700 Series
- Virtualized Packet Core?Distributed Instance (VPC?DI) System Software
- Virtualized Packet Core?Single Instance (VPC?SI) System Software
- Cisco IOS XR 6.3.1, 6.2.3 edo aurreko plataforma guztiak, gutxienez IPv4 laguntza helbide bat konfiguratuta daukatenak gailuaren interfazean.

- Adaptive Security Appliance (ASA) 5500-X Series Firewalls, FirePOWER Services delakoarekin
- Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewalls
- Advanced Malware Protection (AMP) for Networks, 7000 Series Appliances
- Advanced Malware Protection (AMP) for Networks, 8000 Series Appliances
- Firepower 4100, 7000 eta 8000 Series Appliances
- Firepower 2100, 4100 eta 9300 Series Security Appliances
- Firepower Threat Defense for Integrated Services Routers (ISRs)
- Firepower Threat Defense Virtual for VMware
- Industrial Security Appliance 3000
- Sourcefire 3D System Appliances
- Cisco Firepower Threat Defense (FTD) Software 6.2.1 eta 6.2.2. bertsioak.
- 3000 Series Industrial Security Appliances (ISA)
- ASA 5500 Series Adaptive Security Appliances
- ASA 5500-X Series Next-Generation Firewalls
- ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Adaptive Security Virtual Appliance (ASAv)
- Firepower 9300 ASA Security Module
- Firepower Threat Defense Virtual (FTDv)

**Azalpena:**

Cisco produktuei eragiten dieten 11 segurtasun buletin argitaratu dira; horietako bik larritasun kritikoa dute eta beste bederatziek altua.

**Konponbidea:**

Zerbitzu-kontraturen bat indarrean duten erabiltzaileek eguneraketa bat deskargatu dezakezue zuen produktuaren ahultasuna konpontzeko, honakoa helbidean:

- https://software.cisco.com/download/navigator.html

Ez baduzu zerbitzu-kontraturik, mesedez, kontsultatu Cisco TAC zerbitzuarekin:

- https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

**Xehetasuna:**

Larritasun kritikoa duten ahultasunak honakoak dira:

- Kodearen urrutiko exekuzioaren ahultasuna, Cisco WebEx Clients delakoan: Erasotzaile batek ".swf" artxibo gaizto bat bidal dezake bezeroaren artxibo trukerako sistemaren bidez. Bilerara bertaratzen den batek flash artxibo gaizto hori zabaltzean, erasotzaileak kodearen urrutiko exekuzioa lortu dezake. Ahultasun horretarako CVE-2018-0112 identifikatzailea erreserbatu da.
- Informazioa zabaltzeko ahultasuna, Cisco UCS Director Virtual Machine: Roletan oinarritutako baliabideen egiaztatze oker baten ondorioz, sisteman saioa hasten duen egiaztatutako erabiltzaile batek "Baliabide birtualak" menuan agertzen diren makina birtual guztietan ikusgaitasuna eduki dezake eta edozein makina birtualetan baimendutako edozein eragiketa egin. Ahultasun horretarako CVE-2018-0238 kodea erreserbatu da.
- Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2018-0239, CVE-2018-0241, CVE-2018-0233, CVE-2018-0230, CVE-2018-0229, CVE-2018-0240, CVE-2018-0231, CVE-2018-0228 y CVE-2018-0227.

**Etiketak:** Eguneratzea, Cisco, Ahultasuna

---

# Cross Site Scripting ahultasuna Drupal core sisteman

**Argitaratze-data:** 2018/04/19

**Garrantzia:** Media

**Kaltetutako baliabideak:**

- Drupal 8, 8.5.2 edo 8.4.7 bertsioen aurrekoak.
- Drupal 7, baldin eta CKEditor instalatu bazen CDN ez zen metodoren bat erabilita eta erabiltzen den CKEditorren bertsioa 4.5.11 eta 4.9.1 bitartekoa bada.

**Azalpena:**

CKEditor garapen ekipoak cross site scripting motako ahultasun bat antzeman du, testu editorean. Kritikotasun maila tartekoa da.

**Konponbidea:**

- Drupal 8:
  - Drupal 8.5.2 o Drupal 8.4.7 bertsiora eguneratzea.
- Drupal 7, baldin eta CKEditor instalatzen bada CDN ez den metodoren bat erabilita eta erabiltzen den CKEditorren bertsioa 4.5.11 eta 4.9.1 bitartekoa bada.
  - CKEditor a 4.9.2 bertsiora eguneratzea.

**Xehetasuna:**

Drupalen barruan dagoen hirugarrenen JavaScript liburutegi bateko ahultasun baten ondorioz, erasotzaileren bat sar liteke erabiltzaile baimenekin eta cross site scripting motako eraso bat egin, CKEditor-en.

**Etiketak:** Eguneratzea, Edukien kudeatzailea, Ahultasuna

---

# Alderantzizko proxy Squid ahultasuna

**Argitaratze-data:** 2018/04/20

**Garrantzia**: Handia

**Kaltetutako baliabideak:**

Hurrengo produktuek ahultasunen bat daukate alderantzizko proxy gisa erabiltzen direnean:

- Squid-3.1.12.2 eta Squid-3.1.23 bitarteko bertsioak, biak barne, "--enable-esi" eta "--enable-ssl" aukerak aktibatuta.
- Squid-3.2.0.8 eta Squid-3.2.14 bitarteko bertsioak, biak barne, "--enable-esi" eta "--enable-ssl" aukerak aktibatuta.
- Squid-3.3 eta Squid-3.3.14 bitarteko bertsioak, biak barne, "--enable-esi" eta "--enable-ssl" aukerak aktibatuta.
- Squid-3.4 eta Squid-3.4.14 bitarteko bertsioak, biak barne, "--enable-esi" eta "--enable-ssl" aukerak aktibatuta.
- Squid-3.5 eta Squid-3.5.27 bitarteko bertsioak, biak barne, "--enable-esi" eta "--enable-ssl" aukerak aktibatuta.
- Squid-4 eta Squid-4.0.12 bitarteko bertsioak, biak barne, "--with-openssl" aukera aktibatuta.

**Azalpena:**

Trend Micro-ko Michael Marshallek Squiden bertsio batzuetan antzemandako ahultasun baten berri eman du, alderantzizko proxyaren funtzionalitatea erabiltzen den kasuetan. Erasotzaile batek zerbitzua ukatzeko aukera izan dezake, punteroa modu okerrean erabiliz, ESI erantzunak prozesatzean.

**Konponbidea:**

Ahultasun hori Squid 4.0.13 bertsioan zuzendu da.

Gainera, bertsio egonkorretan arazo hori konpontzen duten eguneraketak eskuragarri daude partxeen biltegian:

- Squid 3.5: http://www.squid-cache.org/Versions/v3/3.5/changesets/SQUID-2018_3.patch

Aurretik paketatutako Squid programaren bertsioetarako, kontsultatu zure hornitzailearekin, eguneraketen eskuragarritasunaz informazio gehiago izateko.

**Xehetasuna:**

Ahultasun bat dago ClientRequestContext::sslBumpAccessCheck() delakoaren barruan. Horren ondorioz, bereziki diseinatutako eskaera batek puntero baliogabe baten erreferentzia eza ekar lezake. Horren ondorioz, egiaztatu gabeko urrutiko erasotzaile batek zerbitzua ukatuko du Squiden instalazio ahuletan. Ahultasun horretarako CVE-2018-1172 kodea erreserbatu da.

**Etiketak:** Eguneratzea, Ahultasuna

---

# Kodearen urrutiko exekuzioaren ahultasuna Drupalen core delakoan

**Argitaratze-data:** 2018/04/26

**Garrantzia:** Kritikoa

**Kaltetutako baliabideak:**

Drupalen kaltetutako bertsioak:

- 7.x
- 8.x

**Azalpena:**

Drupalen Segurtasun Taldeak ahultasun kritiko bat atzeman du Drupalen core delakoan. Ahultasun horren ondorioz, urrutiko erasotzaile batek Drupalen oinarritutako web eremu bat kolokan jar dezake.

**Ebazpena:**

Drupalek hainbat eguneraketa argitaratu ditu, bertsioaren arabera erabiltzeko. Drupalen azken bertsiora eguneratzea gomendatzen da:

- 7.x bertsioa erabiltzekotan, eguneratu eta jarri Drupal 7.59.
- 8.4.x bertsioa erabiltzekotan, eguneratu eta jarri Drupal 8.4.8.
- 8.5.x bertsioa erabiltzekotan, eguneratu eta jarri Drupal 8.5.3.

Berehala eguneratu ezin izatekotan edo gaitutakoen artean ez dagoen Drupal bertsio bat izatekotan, ahultasun hori konpontzeko segurtasun-partxea deskargatu eta aplikatu dezakezu:

- Partxea Drupal 8.x.
- Partxea Drupal 7.x.

**Xehetasuna:**

Ahultasun horren ondorioz, urrutiko erasotzaile batek Drupalen oinarritutako web eremu bat kolokan jar dezake, hainbat eraso bektore erabiliz. Ahultasun horretarako CVE-2018-7602 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, Ahultasuna

---

# Hainbat ahultasun IBMren BigFix Platform sisteman

**Argitaratze-data:** 2018/04/27

**Garrantzia:** Alta

**Kaltetutako baliabideak:**

BigFix Platform bertsio hauek:

- 9.2.
- 9.5.

**Azalpena:**

Hainbat ahultasun atzeman dira BigFix Platform sisteman; hiru tarteko kritikotasuna dutenak eta bat kritikotasun altukoa.

**Konponbidea:**

Ahultasun horiek konpontze aldera, hainbat partxe argitaratu dira, bertsioaren araberakoak:

- BigFix Platform 9.2 bertsiorako, 14 partxea.
- BigFix Platform 9.5 bertsiorako, 9 partxea.

**Xehetasuna:**

Larritasun handiko ahultasuna BigFix Relay Diagnostic orrian egindako egiaztatze-saiakeren kudeaketa txar bat izan da. Erasotzaile batek hiztegi eraso bat edo indarrezkoa egin lezake. Ahultasun horretarako CVE-2018-1475 identifikatzailea erreserbatu da.

**Etiketak:** Eguneratzea, IBM, Ahultasuna

---

# Hainbat ahultasun PHP sisteman

**Argitaratze-data:** 2018/04/27

**Garrantzia:** Handia

**Kaltetutako baliabideak:**

- PHP 7.2.x
- PHP 7.1.x
- PHP 7.0.x
- PHP 5.6.x

**Azalpena:**

Segurtasun-ahultasun batzuk konpontzen dituzten PHPren hainbat bertsio argitaratu dira.

**Konponbidea:**

PHP eguneratzea, bertsio hauetako batean instalatutako produktu-adarraren arabera:

- PHP 7.2.5
- PHP 7.1.17
- PHP 7.0.30
- PHP 5.6.36

**Xehetasuna:**

Eguneratuz, kaltetutako bertsioetako akatsak konpon daitezke, baita honako ahultasunak zuzendu ere:

- Memoria dinamikoaren pilaren bufferrak gainezka egitea (heap).
- Ustekabean ixtea, bereziki diseinatutako LDAP erantzunaren ondorioz.
- CVE-2018-5712 guztiz zuzenduta dago.

**Etiketak:** Eguneratzea, PHP, Ahultasuna