2018ko Ekainaren Bulletina

Ohartarazpenak - Teknikoak

IBMren InfoSphere Information Server-en pribilegioen eskalatzea

Argitalpen data: 2018/06/04

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM Information Server Framework: 9.1, 11.3, 11.5 eta 11.7 bertsioak
- IBM InfoSphere Information Server Cloud, 11.5 eta 11.7 bertsioak

Azalpena:

IBMk kritikotasun altuko ahultasun bat aurkitu du, erasotzaile bati pribilegioak eskalatzea ahalbidetu liezaiokeena.

Konponbidea:

IBMk aholkatzen du kaltetutako produktuak eskuragarri dagoen azken bertsiora eguneratzea:

- IBM InfoSphere Information Server 11.7.0.1 bertsioa
- IBM InfoSphere Information Server 11.5.0.2 bertsioa
  IBM InfoSphere Information Server Framework segurtasun partxea

Xehetasuna:

IBM InfoSphere Information Server-ek ahalbidetu lezake erabiltzaile batek pribilegioen eskalatze bat egitea, horren bidez administrari baimenak lortuz, sarbide kontrolak okerrak direlako. Ahultasun horretarako CVE-2017-1350 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2018/06/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco Prime Collaboration Provisioning (PCP), 12.2 bertsioa eta lehenagokoak
- Cisco AsyncOS, WSA softwarearen 10.5.1, 10.5.2 eta 11.0.0 bertsioak
- Cisco Network Services Orchestrator (NSO), 4.1etik 4.1.6.0ra bitarteko bertsioak; 4.2tik 4.2.4.0ra bitartekoak; 4.3tik 4.3.3.0ra bitartekoak eta 4.4tik 4.4.2.0ra bitartekoak
- Cisco IP Phone 6800, 7800 eta 8800, 11.1(2) baino lehenagoko multiplataforma firmwareren bertsioa dutenak
- Prime Collaboration Assurance eta Prime Collaboration Provisioning produktuak.
- Cisco Voice Operating System-en (VOS) oinarritutako ondoko produktuak:
  - Emergency Responder.
  - Finesse.
  - Hosted Collaboration Mediation Fulfillment.
  - MediaSense.
  - Prime License Manager.
  - SocialMiner.
  - Unified Communications Manager (UCM).
  - Unified Communications Manager IM and Presence Service (IM&P) (aurreko bertsioak Cisco Unified Presence izenaz ezagutzen ziren).
  - Unified Communication Manager Session Management Edition (SME).

    - Unified Contact Center Express (UCCx).
    - Unified Intelligence Center (UIC).
    - Unity Connection eta Virtualized Voice Browser.
- Cisco Meeting Server (CMS) 2000 Platforms, CMS Softwarearen 2.2.13 edo 2.3.4 bertsioak baino lehenagokoak exekutatzen
- Cisco ASA Software eta Cisco Firepower Threat Defense (FTD) Software, ondoko produktuen gainean:
    - 3000 Series Industrial Security Appliance (ISA).
    - ASA 1000V Cloud Firewall.
    - 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 2100 Series Security Appliance.
    - Firepower 4100 Series Security Appliance.
    - Firepower 9300 ASA Security Module.
    - FTD Virtual (FTDv).
- Cisco Unified IP Phone software.
- Cisco WebEx.
- Cisco Wide Area Application Services (WAAS) Software, berezko konfigurazioarekin.
- Cisco Integrated Management Controller Supervisor Software eta Cisco UCS Director Software.
- Cisco Unified Computing System (UCS) Software.
- Cisco Prime Collaboration Provisioning.
- Cisco Identity Services Engine (ISE).
- Cisco Unified Communications Manager.
- Cisco Unity Connection.
- Cisco FireSIGHT System Software.
- Cisco AnyConnect Network Access Manager eta Cisco AnyConnect Secure Mobility Client for iOS, Mac OS X, Android, Windows and Linux

Azalpena:

Ciscok hainbat produkturi buruzko 28 ahultasun argitaratu ditu, horietatik 2 larritasun kritikokoak, 11 larritasun altukoak eta 15 larritasun ertainekoak.

Konponbidea:

Ciscok erabiltzaileen eskura jarri ditu hainbat eguneraketa, kaltetutako produktuaren arabera. Hemendik jaits daitezke ahultasunak konpontzen dituzten eguneraketak:

- Software Ciscoren deskarga panela

Xehetasuna:

Honakoak dira larritasun kritikoko ahultasunak:

- Network Interface and Configuration Engine (NICE) zerbitzuko ataka ireki batean dagoen ahultasun bat, erasotzaile batek balia lezakeena, eragindako PCP instantzia batean irekitako RMI sistemara sarbidea lortuz. PCPa eta berari lotutako gailuak kaltetzeko ekintza gaiztoak egin litezke. Ahultasun horretarako CVE-2018-0321 identifikatzailea erreserbatu da.
- Memoria eragiketa okerren ondorioz gertatutako ahultasuna, kaltetutako softwareak saioa hasteko autentifikazioaren unean erabiltzaile izen bat analizatzen duenean. Ahultasun hori baliatuz erasotzaile batek gailuan kode arbitrarioa exekuta lezake edo bere gainkarga eragin, ondorioz zerbitzuaren ukapen egoera sortuz (DoS). Ahultasun horretarako CVE-2018-0315 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2018-0353, CVE-2018-0320, CVE-2018-0318, CVE-2018-0319, CVE-2018-0317, CVE-2018-0322, CVE-2018-0274, CVE-2018-0316, CVE-2017-6779, CVE-2018-0263, CVE-2018-0296, CVE-2018-0332, CVE-2018-0357, CVE-2018-0356, CVE-2018-0329, CVE-2018-0352, CVE-2018-0149, CVE-2018-0338, CVE-2018-0340, CVE-2018-0336, CVE-2018-0339, CVE-2018-0355, CVE-2018-0354, CVE-2018-0335, CVE-2018-0333, CVE-2018-0334.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun IBMren Security Identity Manager-en

Argitalpen data: 2018/06/08

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM Security Identity Manager, 7.0 eta 7.0.1 bertsioak.

Azalpena:

IBMk 5 ahultasun aurkitu ditu: bat kritikotasun altukoa, beste bi kritikotasun ertainekoak eta gainerako biak kritikotasun txikikoak.

Konponbidea:

Kaltetutako produktuaren arabera, konponbideak ezberdinak dira:

- 7.0 bertsioa: IBMren laguntza zerbitzuarekin harremanetan jarri.
- 7.0.1 bertsioa: 7.0.1-ISS-SIM-FP0009 eguneraketa jaitsi.

Xehetasuna:

Kritikotasun altuko ahultasun hau baliatuz, autentifikatutako erasotzaile batek fitxategi gaiztoak igo litzake, eremuan automatikoki prozesatuak izan litezkeenak. Ahultasun horretarako CVE-2018-1453 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Ahultasunak Asterisk produktuetan

Argitalpen data: 2018/06/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Asterisk Open Source:
  - 13.x, 13.10.0 bertsioa eta aurrekoak.
  - 14.x bertsio guztiak.
  - 15.x bertsio guztiak.
- Certified Asterisk 13.18 eta 13.21 bertsio guztiak.

Azalpena:

Asteriskek bi segurtasun buletin argitaratu ditu, bat larritasun kritikokoa eta bestea baxukoa. Horiek baliatuz erasotzaile batek zerbitzu ukapen egoera sor lezake edo informazio konfidentzialera sarbidea izan.

Konponbidea:

Asteriskek kaltetutako produktuak eguneratzea aholkatzen du:

- Asterisk Open Source, 15.4.1, 13.21.1 eta 14.7.7 bertsioetara eguneratzea.
- Certified Asterisk, 13.18-cert4 eta 13.21-cert2 bertsioetara eguneratzea.

Xehetasuna:

TCP/TLS bidez Asteriskera konexio bat egiten denean, eta bezeroa bat-batean deskonektatzen denean, edo bereziki diseinatutako mezu bat bidaltzen duenean, zerbitzua begizta amaigabean sartzea eragin dezake, zerbitzuaren ukapen egoera sortuz.

Etiketak: Eguneraketa, Ahultasuna

VMwareren AirWatch Agent-en ahultasuna

Argitalpen data: 2018/06/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- VMware AirWatch Agent Androiderako (A/W Agent)
- VMware AirWatch Agent Windows Mobilerako (A/W Agent)

Azalpena:

Ahultasun kritiko bat aurkitu da, eta horren bitartez urruneko erasotzaile batek kodea exekutatu, baimenik gabe fitxategiak sortu eta exekutatu eta direktorio publikoetara sarbidea izan lezake.

Konponbidea:

VMwarek hainbat eguneraketa argitaratu ditu, kaltetutako gailuaren arabera:

- Android gailuetarako, aplikazioa AirWatch Agent 8.2 bertsiora eguneratzea, Google Play-en eskuragarri.
- Windows Mobile gailuetarako, aplikazioa Agent 6.5.2 bertsiora eguneratzea, lotura honetan eskuragarri.

Xehetasuna:

Ahultasun hori baliatuz urruneko erasotzaile batek kodea exekuta lezake, eta denbora errealean fitxategien kudeatzailea erabili, bai eta Agent sandbox-en fitxategiak baimenik gabe sortu eta exekutatu ere. Era berean, asmo txarreko administrari bat direktorio publikoetara sar liteke, esate baterako, SD txartelekoetara. Ahultasun horretarako CVE-2018-6968 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

2018ko ekaineko Microsoften segurtasun buletina

Argitalpen data: 2018/06/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Internet Explorer.
- Microsoft Edge.
- Microsoft Windows.
- Microsoft Office y Microsoft Office Services eta Web Apps.
- ChakraCore.
- Adobe Flash Player.

Azalpena:

Microsoftek hilean behin segurtasun eguneraketei buruz argitaratzen duen argitalpeneko hile honetako alean 50 ahultasun jaso dira. Horietatik 10 kritiko gisa sailkatu dira eta 40 garrantzitsu gisa. Gainerako ahultasunak larritasun baxu edo ertainekoak dira.

Konponbidea:

Dagokion eguneraketa instalatzea. Segurtasun eguneraketen instalazioei buruzko informazio orrian eguneraketa metodo ezberdinei buruz

informatzen da.

Xehetasuna:

Ekainari dagokion segurtasun eguneraketen buletinean hainbat segurtasun ahultasun argitaratu dira, mota hauetakoak:

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

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

---

SAPen segurtasun eguneraketa 2018ko ekainean

Argitalpen data: 2018/06/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business One, 9.2 eta 9.3 bertsioak
- SAP Internet Sales, 7.30,7.31, 7.32, 7.33 eta 7.54 bertsioak
- SAP Business Objects CMC, BI Launchpad, Friorified BI Launchpad, 4.0, 4.10, 4.20 eta 4.30 bertsioak
- SAP Business Objects Enterprise, 4.0 eta 4.1 bertsioak
- SAP UI5
- SAP UI5 Handler
- SAP Identity Management, 8.0 bertsioa

Azalpena:

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

Konponbidea:

SAPen laguntzarako webgunea bisitatu eta fabrikatzaileak adierazten dituen beharrezko eguneraketa edo partxeak instalatzea.

Xehetasuna:

SAPek segurtasun partxeei buruz argitaratzen duen hileroko komunikatuan 10 segurtasun ohar eman ditu ezagutzera. Horietatik 3 ohar lehenagotik argitaratutako segurtasun oharrei dagozkien eguneraketak dira. Hamar horietatik 2 larritasun kritikokoak dira, beste 4 larritasun altukoak eta beste 4 larritasun ertainekoak.

Argitaratutako ahultasun motak ondoko hauek dira:

- Kode injekzioko 2 ahultasun
- Informazio zabalkundeko 2 ahultasun
- Zerbitzuaren ukapeneko ahultasun bat
- Cross-Site Scripting gabezia erako ahultasun bat
- XMLren balioztatze okerreko ahultasun bat
- Beste tipologia batzuetako 3 ahultasun

Ahultasun garrantzitsuenak ondoko hauek dira:

- SAP Business One-n informazio zabalkundea, erasotzaile bati informazio gehigarria eskuratzen lagunduko liokeena (sistemaren datuak, arazketa informazioa, eta abar). Horren bitartez sistemari buruz ikasi ahal izango luke eta beste eraso batzuk planifikatu ahal izango lituzke.
- Baimenik gabeko erasotzaile batek urrunetik komandoak exekutatu ahal izango lituzke hura exekutatu zuen zerbitzuaren pribilegio maila berdinekin. Hartara, SAP zerbitzari bateko fitxategi sistema batean kokatutako fitxategi eta direktorio arbitrarioetara sarbidea izango luke, esate baterako, aplikazioaren iturri kodera, konfiguraziora edo sistemako fitxategi kritikoetara. Horrela informazio tekniko kritikoa eta negozioari buruzkoa lor lezake.
- Erasotzaile batek SAP Internet Sales-en zerbitzuaren ukapeneko ahultasun bat erabil lezake osagai ahul baten prozesu bat amaitzeko, inork erabil dezan eragotziz. Horrek negozio prozesuei, sistemaren erabilgarritasunari eta, beraz, negozioaren ospeari eragingo lioke.

Etiketak: Eguneraketa, SAP, Ahultasuna

Pribilegioen eskalatzea IBM Netezza plataforman

Argitalpen data: 2018/06/15

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM Netezza Platform Software, 7.0.4tik 7.2.1.6ra bitarteko bertsioak

Eragina:

Pribilegio alturik gabeko eta asmo txarreko erabiltzaile batek supererabiltzaile modura komandoak exekuta litzake kaltetutako produktuetan.

Konponbidea:

Fabrikatzaileak argitaratutako hurrengo bertsiora eguneratzea:

IBM Netezza Platform Software v7.2.1.6-P1

Xehetasuna:

Erabiltzaile lokal batek globalki editagarria den fitxategi bat alda lezake, eta horrela root erabiltzaile modura komandoak exekutatzeko erabil liteke. Ahultasun horretarako CVE-2018-1460 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM

Urruneko sarbide ez baimendua HPE NFVDn

Argitalpen data: 2018/06/19

Garrantzia: Handia

Kaltetutako baliabideak:

HPE Network Function Virtualization Director (NFVD), 4.2.1 bertsioa, 3 gui partxea baino lehenagokoak.

Azalpena:

HPEk ahultasun bat identifikatu du HPE Network Function Virtualization Director (NFVD) produktuan. Horren bitartez lor liteke urruneko sarbidea eta baimenik gabeko irismena informazio sentikorrera.

Konponbidea:

- NFVD 4.2.1-en gui 3 partxea aplikatzea.

Xehetasuna:

Urruneko sarbide ez baimenduen erako ahultasun bat identifikatu da, eta hori baliatuz urrunetik informazio sentikorrera sartzea lor liteke. Ahultasun horretarako CVE-2018-7071 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, HP

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2018/06/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- MDS 9000 Series Multilayer Switches
- Nexus 2000 Series Fabric Extenders
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Line Cards and Fabric Modules
- Firepower 4100 Series Next-Generation Firewalls
- Firepower 9300 Security Appliance
- UCS 6100 Series Fabric Interconnects
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- Nexus 3600 Platform Switches
- Nexus 2000 Series Switches
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode
- Nexus 1000V Series Switches
- Nexus 1100 Series Cloud Services Platforms
- Nexus 4000 Series Switches
- Firepower 4100 Series Next-Generation Firewall
- MDS 9000 Series Multilayer Director Switches
- Nexus 9000 Series Switches in NX-OS mode
- Firepower 2100 Series
- Nexus 4000 Series Switch
- Cisco TelePresence Video Communication Server (VCS) Expressway
- Cisco Unified Communications Manager IM & Presence Service
- Cisco Unified Communications Domain Manager
- Cisco NX-OS Software.
- Acano X-Series
- Cisco Meeting Server 1000
- Cisco Meeting Server 2000
- Cisco Firepower Management Center
- Cisco 5000 Series Enterprise Network Compute System
- Cisco UCS E-Series Servers
- Cisco Meeting Server
- Cisco AnyConnect Secure Mobility Client for Windows Desktop

Azalpena:

Ciscok hainbat produkturi buruzko 22 ahultasun argitaratu ditu, horietatik 5 larritasun kritikokoak, 19 larritasun altukoak eta 9 larritasun ertainekoak.

Konponbidea:

Ciscok erabiltzaileen eskura jarri ditu hainbat eguneraketa, kaltetutako produktuaren arabera. Hemendik jaits daitezke ahultasunak konpontzen dituzten eguneraketak:

-

Xehetasuna:

Honakoak dira larritasun kritikoko ahultasunak:

- NX-API azpisistemaren autentifikazio moduluan sartzeko parametroetako balioztatze oker baten ondoriozko ahultasun batek ahalbidetu lezake autentifikaziorik gabeko urruneko erasotzaile batek aldatutako HTTP edo HTTPS pakete bat bidaltzea kaltetutako sistemaren kudeaketa interfazera, NX-API ezaugarria gaituta. Pakete horrek eragin lezake kodea exekutatzea root baimenekin. Ahultasun horretarako CVE-2018-0301 identifikatzailea erreserbatu da.
- Cisco Fabric Services paketeetako goiburuetan balioen balioztatze ez aski batek eragindako ahultasunak autentifikaziorik gabeko urruneko erasotzaile bati ahalbidetu liezaioke aldatutako pakete bat sortzea eta kaltetutako gailura bidaltzea. Pakete horrek bufferra gainezkatzea lor lezake, kode arbitrarioa exekutatzea edo zerbitzua ukatzea (DoS) eraginez. Ahultasun horretarako CVE-2018-0308 identifikatzailea erreserbatu da.
- Cisco Fabric Services osagaiaren ahultasun batek ahalbidetu lezake autentifikaziorik gabeko urruneko erasotzaile batek aldatutako pakete bat bidaltzea, eta bufferraren gainezkatzea edo bere gainirakurketa eragitea; horren ondorioz, memoriaren edukia irakurtzea, zerbitzua ukatzea (DoS) edo root baimeneko mailarekin kodea exekutatzea ahalbidetuz. Ahultasun horretarako CVE-2018-0304 identifikatzailea erreserbatu da.
- Cisco Fabric Services paketeetako goiburuak prozesatzean balioztatze ez aski batek eragindako ahultasunak autentifikaziorik gabeko urruneko erasotzaile bati ahalbidetu liezaioke aldatutako pakete bat sortzea. Pakete hori prozesatzeak bufferra gainezkatzea eragin lezake, eta horrekin batera kode arbitrarioa exekutatzea eragin liteke. Ahultasun horretarako CVE-2018-0314 identifikatzailea erreserbatu da.
- Cisco Fabric Services paketeetako goiburuak prozesatzean balioztatze ez aski batek eragindako ahultasunak autentifikaziorik gabeko urruneko erasotzaile bati ahalbidetu liezaioke aldatutako pakete bat sortzea. Pakete hori prozesatzeak bufferra gainezkatzea eragin lezake, eta horrekin batera kode arbitrarioa exekutatzea edo zerbitzua ukatzea (DoS) eragin liteke. Ahultasun horretarako CVE-2018-0312 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2018-0307, CVE-2018-0291, CVE-2018-0293, CVE-2018-0292, CVE-2018-0295, CVE-2018-0294, CVE-2018-0330, CVE-2018-0331, CVE-2018-0311, CVE-2018-0310, CVE-2018-0306, CVE-2018-0313, CVE-2018-0299, CVE-2018-0309, CVE-2018-0298, CVE-2018-0302, CVE-2018-0303, CVE-2018-0305, CVE-2018-0300, CVE-2018-0358, CVE-2018-0363, CVE-2018-0364, CVE-2018-0337, CVE-2018-6242, CVE-2018-0365, CVE-2018-0362, CVE-2018-0359, CVE-2018-0373.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun Netgear-en produktuetan

Argitalpen data: 2018/06/26

Garrantzia: Handia

Kaltetutako baliabideak:

Argitaratutako ahultasunek Netgear-en router, atebide eta anplifikadore modelo batzuei eragiten diete.

Kaltetutako produktuen zerrenda osoa beherago ikus daiteke, Erreferentziak atalean.

Azalpena:

Netgear-ek konponbideak argitaratu ditu bere produktuetako batzuei eragiten dieten larritasun altu eta ertaineko hainbat ahultasunetarako.

Konponbidea: Netgear-en laguntzarako webgunetik jaits daiteke produktu bakoitzerako eskuragarri dagoen firmwarearen azken bertsioa. https://www.netgear.com/support/.

Xehetasuna:

Hauek dira Netgear-ek konpondu dituen ahultasun motak:

- Segurtasun konfigurazio okerra
- Cross-Site Request Forgery (CSRF)
- Komandoen injekzioa autentifikazioaren ondoren
- Bufferraren gainezkatzea autentifikazioaren aurretik eta ondoren
- Informazio sentikorra ezagutzera ematea
- Zerbitzua ukatzea

Etiketak: Eguneraketa, Pribatutasuna, Ahultasuna

Joomla! edukien kudeatzailean ahultasunak

Argitalpen data: 2018/06/27

Garrantzia: Txikia

Kaltetutako baliabideak:

- Joomla! 1.6.0tik 3.8.8ra bitarteko bertsioak

Azalpena:

Joomla! edukien kudeatzaileak ahultasuna izan lezake XSS injekzio baten edo fitxategien inklusio lokal baten kasuetan.

Konponbidea:

Azken bertsiora eguneratzea:

- Joomla! 3.8.10

Xehetasuna:

- Uneko hizkuntzarako loturak filtratu gabeko HTML karaktere bereziak izan litzake, eta horrek erasotzaile bati ahalbidetuko lioke XSS islatu bat egitea.
- "Class_exists" funtzioak ez ditu egiten egiaztapen egokiak, eta horren ondorioz, erasotzaile batek fitxategien inklusio lokal bat egin lezake.

Etiketak: Eguneraketa, Edukien kudeatzailea, Ahultasuna

Hewlett Packard-en iLO-n baimendu gabeko urruneko aldaketa

Argitalpen data: 2018/06/27

Garrantzia: Handia

Kaltetutako baliabideak:

- HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers ? v1.30 baino lehenagokoa
- HPE Integrated Lights-Out 4 (iLO 4) ? v2.60 baino lehenagokoa

Azalpena:

Hewlett Packard Enterprisek (HPE) larritasun altuko ahultasun baten berri eman du. Horren eraginez, eragindako produktuetan erasotzaile batek informazioa alda lezake baimenik gabe.

Konponbidea:

HPEk erabiltzaileen eskura jarri ditu ahultasuna konpontzen duten firmwarearen ondoko bertsioak:

- iLO 4 v2.60
- iLO 5 v1.30

https://support.hpe.com/hpesc/public/home webgunetik jaits daitezke firmwarearen eguneraketak

Xehetasuna:

Urruneko erasotzaile batek HPren iLO urruneko kudeaketako mekanismoaren ahultasun bat balia lezake eta horren bidez informazioa alda lezake baimenik gabe. Ahultasun horretarako, CVE-2018-7078 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, HP, Eguneraketa

Hainbat ahultasun IBMren Rational DOORSen

Argitalpen data: 2018/06/27

Garrantzia: Handia

Kaltetutako baliabideak:

- Rational DOORS: 9.5.1 - 9.5.1.9
- Rational DOORS: 9.5.2 - 9.5.2.8
- Rational DOORS: 9.6.0 - 9.6.0.7
- Rational DOORS: 9.6.1 - 9.6.1.10
- Rational DOORS desktop client
- Rational DOORS interoperation server

Azalpena:

Rational DOORSen hiru ahultasun aurkitu dira, bat larritasun altukoa eta beste bi larritasun ertainekoak. Hainbat arazo eragin litzakete: administrazio baimenak eskuratzea, pasahitz ahulak berreskuratzea edo zerbitzua ukatzea.

Konponbidea:

- Rational DOORSen 9.5.1 - 9.5.1.9 bertsioetarako, bertsio honetara eguneratzea: 9.5.1.10
- Rational DOORSen 9.5.1 - 9.5.1.9 bertsioetarako, bertsio honetara eguneratzea: 9.5.2.9
- Rational DOORSen 9.5.1 - 9.5.1.9 bertsioetarako, bertsio honetara eguneratzea: 9.6.0.8
- Rational DOORSen 9.5.1 - 9.5.1.9 bertsioetarako, bertsio honetara eguneratzea: 9.6.1.11

Xehetasuna:

- Larritasun altuko ahultasunak erasotzaile bati administrazio baimenak eskuratzea ahalbidetuko lioke. Ahultasun horretarako CVE-2018-1457 kodea erreserbatu da.
- GSKit CMSren KDBaren hash funtzioak duen akatsaren ondorioz pasahitzen babesa aurreikusitakoa baino ahulagoa da. Erasotzaile batek egoera hori balia lezake pasahitz ahul bat berreskuratzeko. Ahultasun horretarako CVE-2018-1447 kodea erreserbatu da.
- IBM GSKitek inguruneko hainbat aldagai ditu erasotzaile batek gaindi litzakeenak, eta horren bitartez zerbitzuaren ukazioa eragin. Ahultasun horretarako CVE-2018-1427 kodea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun VMwareren zenbait produktutan

Argitalpen data: 2018/06/29

Garrantzia: Handia

Kaltetutako baliabideak:

- VMware vSphere ESXi (ESXi) 14.x bertsioak
- VMware Workstation Pro / Player (Workstation) 14.x bertsioak
- VMware Fusion Pro, Fusion (Fusion) 10.x bertsioak

Azalpena:

WMwarek mugez kanpoko irakurketa erako hainbat ahultasunen berri eman du. Bere ESXi, Workstation eta Fusion produktuei eragiten diete, eta informazioaren zabalkundea edo ustekabeko itxiera izan lezakete ondoriotzat.

Konponbidea:

Eskuragarri daude ondoko eguneraketak:

- ESXi 6.7
- VMware Workstation Pro 14.1.2
- VMware Workstation Player 14.1.2
- VMware Fusion Pro / Fusion 10.1.2

Xehetasuna:

Shader traslator-en mugez kanpoko irakurketa erako ahultasunek ahalbidetu lezakete baimenik gabeko erabiltzaileek informazioaren zabalkundea edo sistemaren ustekabeko itxiera eragitea. Ahultasun horietarako CVE-2018-6965, CVE-2018-6966 eta CVE-2018-6967 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, VMware, Ahultasuna