2019ko Urriaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun HPEren produktuetan

Argitalpen data: 2019/10/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- HPE UIoT, 1.2.4.2 bertsioa;
- Simplivity OmniCube, 3.0.7tik 3.7.9ra bitarteko bertsioak;
- SimpliVity 380, 3.0.7tik 3.7.9ra bitarteko bertsioak;
- SimpliVity 2600;
- Dell, Lenovo eta Cisco-rako SimpliVity OmniStack.

Azalpena:

HPEren segurtasun erantzunen ekipoak hainbat ahultasun aurkitu ditu fabrikatzailearen zenbait produktutan.

Konponbidea:

- UIoTren kasuan, 1.2.4.2 eta lehenagoko bertsioak, 1.2.4.2 RP3 HF1era eguneratzea;
- Simplivity-ren kasuan, OmniStack eguneratzea 3.7.10 bertsiora.

Xehetasuna:

- HPE UIoT-ek daukan ahultasun bat baliatuz, urruneko erasotzaile batek baimenik gabeko sarbidea lor lezake, edo erabiltzailearen informazio konfidentziala ezagutzera eman. Ahultasun horretarako CVE-2019-11995 identifikatzailea erreserbatu da.
- SimpliVity-ren hainbat bertsiotan aurkitutako ahultasun bat baliatuz, erasotzaile batek, bai modu lokalean eta bai urrunetik, nodoetan fitxategi arbitrarioen aldaketak edo ezabaketak egin litzake *root* pribilegioekin, zaharkituta dauden APIetara deiak eginez. Ahultasun horretarako CVE-2019-11993 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, HP, IoT, Ahultasuna

Hainbat ahultasun IBMren Security Directory Server-en

Argitalpen data: 2019/10/02

Garrantzia: Altua

Kaltetutako baliabideak:

Security Directory Server, 6.4.0 bertsioa.

Azalpena:

IBMren *X-Force Ethical Hacking* ekipoak bost ahultasun aurkitu ditu, hiru kritikotasun altukoak eta bi kritikotasun ertainekoak. Urruneko erasotzaile batek informazio sentikorra ezagutzera eman lezake, fitxategiak aldatu, kredentzialak lapurtu edo sistemaren informazioa eskuratu.

Konponbidea:

6.4.0.19-ISS-ISDS-IF0019 bertsiora eguneratzea.

Xehetasuna:

Kritikotasun altuko ahultasunak honako hauek dira:

Kontua ixteko ezarpenen erabilera desegoki bat baliatuz, urruneko erasotzaile batek erabiltzailearen kontuko informazioa eskura lezake indar hutseko erasoen bidez. Ahultasun horretarako CVE-2019-4520 identifikatzailea erreserbatu da.

Birbideratze irekiko eraso bat baliatuz, urruneko erasotzaile batek *phishing* bat egin lezake, eta biktima konbentzitu informazio sentikorra eskuratzeko. Ahultasun horretarako CVE-2019-4538 identifikatzailea erreserbatu da.

XML fitxategiak prozesatzean, posible da elementu batzuk ondo ez neutralizatzea. Erasotzaile batek XMLetako sintaxian, edukian edo komandoetan aldaketak egin litzake, azken sistemak prozesatuak izan aurretik. Ahultasun horretarako CVE-2019-4539 identifikatzailea erreserbatu da.

Kritikotasun ertaineko ahultasunetarako honako identifikatzaile hauek erreserbatu dira: CVE-2019-4542 eta CVE-2019-4549.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Palo Alto Networks-en produktuetan

Argitalpen data: 2019/10/02

Garrantzia: Altua

Kaltetutako baliabideak:

Zingbox Inspector, 1.280, 1.286, 1.288, 1.294 eta lehenagoko bertsioak.

Azalpena:

Larritasun altuko hainbat ahultasun argitaratu dira. Horiek baliatuz, erasotzaile batek kodea arbitrarioki exekuta lezake, barneratutako kredentzialak erabili, datu basean informazioa txertatu edo autentifikazioa saihestu.

Konponbidea:

1.295 bertsiora edo berriagora eguneratzea.

Xehetasuna:

- Zingbox Inspector CLI-k duen komandoen injekzio erako ahultasuna baliatuz, autentifikatutako erasotzaile batek sistemako komando arbitrarioak exekuta litzake. Ahultasun horretarako CVE-2019-15014 identifikatzailea erreserbatu da.
- Erabiltzaileak softwarean autentifikatu litezke barneratutako kodea duten kredentzialak erabiliz, Zingbox Inspector-en SSHrako sarbidea ez badago murriztuta neurri osagarriekin. Ahultasun horietarako CVE-2019-15015 eta CVE-2019-15017 identifikatzaileak erreserbatu dira.
- Autentifikatutako erabiltzaileek saneatu gabeko komandoak txerta litzakete Zingbox Inspector backend-eko datu basean, eta horrek datu baseari edo sistemari arazoak edo beste kalte batzuk eragin diezazkieke. Ahultasun horretarako CVE-2019-15016 identifikatzailea erreserbatu da.
- Zingbox Inspector-ek ez du autentifikaziorik behar Inspector-eko instantzia bezero ezberdin bati lotzen zaionean. Ahultasun horretarako CVE-2019-15018 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/10/03

Garrantzia: Altua

Kaltetutako baliabideak:

- Cisco ASA Software edo Cisco FTD Software-ren bertsio ahul bat exekutatzen duten Cisco produktuak:
  - FTP ikuskaritza egiteko konfiguratutakoak;
  - SIP ikuskaritza funtzionaltasuna gaituta dutenak;
  - OSPF (Open Shortest Path First) sare protokoloarekin lan egin ahal izateko konfiguratutakoak;
  - LAN-to-LAN edo Remote Access IPsec VPN konexioetarako IKEv1 protokoloa gaituta dutenak:
    - Adaptive Security Virtual Appliance (ASAv);
    - Firepower 2100 Series Appliances;
    - Firepower Threat Defense Virtual (FTDv).
- Cisco ASA Software-ren bertsio ahul bat exekutatzen duten eta Clientless SSL VPN edo AnyConnect SSL VPN gaituta duten Cisco produktuak;
- Cisco Unified Communications Manager eta Manager SME;
- Cisco Unified CM IM&P Service;
- Cisco Unity Connection;
- Cisco FMC Software;
- Cisco FTD Software-ren bertsio ahul bat exekutatzen duten eta multiinstantziaren eragiketa konfiguratuta duten Cisco produktuak:
  - Firepower 4100 Series Security Appliances;
  - Firepower 9300 Series Security Appliances.
- Cisco FXOS Software;
- Ondoko plataformetan exekutatzen diren Cisco FXOS Software eta Cisco FTD Software:
  - Cisco Firepower 1000 Series Appliances;
  - Cisco Firepower 2100 Series Appliances;
  - Cisco Firepower 4100 Series Appliances;
  - Cisco Firepower 9300 Series Appliances.

Azalpena:

Ciscok bere produktuei eragiten dieten larritasun altuko 13 ahultasunen berri eman du.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Software Cisco-ren deskarga paneletik deskarga daitezke.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunen bat balia lezake honako ekintza hauetakoren bat egin ahal izateko:

- zerbitzuaren urruneko ukapena;
- urrunetik CSRF (*Cross-Site Request Forgery*) erasoen exekuzioa;
- komandoen injekzioa *root* pribilegioekin;
- kodearen urruneko exekuzioa;
- edukiontziak saihestea;
- SQL injekzioa.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Baimenen esleipen okerra Dell EMCren hainbat produktutan

Argitalpen data: 2019/10/04

Garrantzia: Altua

Kaltetutako baliabideak:

- Dell EMC Avamar Server, 7.4.1, 7.5.0, 7.5.1, 18.2 eta 19.1 bertsioak;
- Dell EMC Integrated Data Protection Appliance (IDPA), 2.0, 2.1, 2.2, 2.3 eta 2.4 bertsioak.

Azalpena:

Dell EMCren hainbat produktuk larritasun altuko ahultasun bat daukate, baliabide kritikoetarako baimenen esleipen oker erakoa.

Konponbidea:

Dell-ek gomendatzen du *hotfix* ezberdinak aplikatzea, kaltetutako produktuen bertsioaren arabera:

- Dell EMC Avamar Server:
  - 7.4.1;
  - 7.5.0;
  - 7.5.1;
  - 18.2;
  - 19.1.
- Dell EMC Integrated Data Protection Appliance (IDPA):
  - 2.0;
  - 2.1;
  - 2.2;
  - 2.3;
  - 2.4.

Xehetasuna:

Ahultasunaren jatorria baliabide kritikoetarako baimenen esleipen okerra da. Autentifikatutako urruneko erasotzaile batek kaltetutako sistemako segurtasun kopien informazio konfidentziala aldatu edo ezagutzera eman lezake. Ahultasun horretarako CVE-2019-3765 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioen eskalatzearen aurrean ahula de APIa IBMren UNIXerako Sterling Connect:Direct-en

Argitalpen data: 2019/10/07

Garrantzia: Altua

Kaltetutako baliabideak:

- Unixerako IBM Sterling Connect:Direct, honako bertsioak:
  - 6.0.0,
  - 4.3.0,
  - 4.2.0.

Azalpena:

IBMk kritikotasun altuko ahultasun bat aurkitu du. Autentifikatutako urruneko erasotzaile batek baimenik gabeko sarbidea lor lezake sisteman.

Konponbidea:

IBMk ahultasuna konpontzen duten segurtasun eguneraketak argitaratu ditu, kaltetutako bertsioaren arabera.

- Honako bertsioetara eguneratzea:
  - 6.0.0,
  - 4.3.0,
  - 4.2.0.

4.2.0 baino lehenagoko bertsioetarako, IBMk aholkatzen du konponbidea duen bertsio batera eguneratzea.

Xehetasuna:

Ahultasuna gertatzen da Connect:Direct-erako pribilegio mugatuak dituen baimendutako erabiltzaile batek *getuid()* inplementazioa asmo gaiztoko beste batekin ordezten duenean, UNIXerako C/C APIaren bidez. Autentifikatutako urruneko erasotzaile batek zerbitzarira baimenik gabeko sarbidea lor lezake. Ahultasun horretarako CVE-2019-4529 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

SAPen 2019ko urriko segurtasun eguneraketa

Argitalpen data: 2019/10/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP NetWeaver Process Integration:
  - AS2 Adapter, 1.0 eta 2.0 bertsioak;
  - B2B Toolkit, 1.0 eta 2.0 bertsioak.
- SAP Landscape Management enterprise edition, 3.0 bertsioa;
- SAP IQ, 16.1 bertsioa;
- SAP SQL Anywhere, 17.0 bertsioa;
- SAP Dynamic Tiering, 1.0 eta 2.0 bertsioak;
- SAP Customer Relationship Management (Email Management):
  - S4CRM, 100 eta 200 bertsioak;
  - BBPCRM, 700, 701, 702, 712, 713 eta 714 bertsioak.
- SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), 420 eta 430 bertsioak
- SAP Financial Consolidation, 10.0 eta 10.1 bertsioak;
- SAP Kernel (RFC):
  - KRNL32NUC, KRNL32UC, KRNL64NUC, 7.21, 7.21EXT, 7.22 eta 7.22EXT bertsioak;
  - KRNL64UC, 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49 eta 7.73 bertsioak;
  - KERNEL, 7.21, 7.49, 7.53, 7.73 eta 7.76 bertsioak.

Azalpena:

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

Konponbidea:

SAPen zerbitzu ataria bisitatzea, eta fabrikatzaileak adierazten duen moduan beharrezkoak diren eguneraketa edo partxeak instalatzea.

Xehetasuna:

SAPek segurtasun partxeei buruz argitaratzen duen hileroko komunikatuan 7 segurtasun ohar eta eguneraketa bat argitaratu ditu. Horietatik 2 larritasun kritikokoak dira, 1 larritasun altukoa eta beste 5 larritasun ertainekoak.

Argitaratutako ahultasun motak honako hauek dira:

- *Cross-Site Scripting* (XSS) erako 3 ahultasun;
- zerbitzuaren ukazioko ahultasun bat;
- informazioaren zabalkunde erako ahultasun bat;
- baimenaren egiaztapen gabeziako ahultasun bat;
- autentifikazio faltako ahultasun bat;
- beste era bateko ahultasun bat.

Kritikotzat eta altutzat kalifikatutako segurtasun oharrak honakoari buruzkoak dira:

- AS2 egokitzailearen konfigurazioak bi segurtasun hornitzaile ezberdin onartzen ditu. Aukeratutako hornitzailearen arabera, autentifikazio gabezi erako ahultasun bat dago. Horrek datu konfidentzialen lapurreta edo manipulazioa ahalbidetu dezake, bai eta administratzaile funtzionaltasunetara eta pribilegioak behar dituzten beste funtzio batzuetara sarbidea izatea ere. Ahultasun horretarako CVE-2019-0379 identifikatzailea erabili da.

- SAP Landscape Management Enterprise-k eragiketa pertsonalizatuen definizioa ahalbidetzen du, horietako bakoitza hornitzaile jakin bati esleituta. Era berean, hornitzaile horri parametro pertsonalizatu gehiago gehitzeko aukera dago. Produktu hau ahula da informazio zabalkundearen aurrean, parametro pertsonalizatu horiek baldintza jakin batzuk betetzen badituzte. Ahultasun horretarako CVE-2019-0380 identifikatzailea erabili da.

- Fitxategien bilaketa algoritmoak ahultasun bat dauka, produktu ezberdinei eragiten diena. Algoritmoak direktorio gehiegitan bilatzen du, baita aplikazioaren eremutik kanpo daudenetan ere. Ahultasun hori baliatuz gero erasotzaile batek sistemako fitxategi arbitrarioak irakurri, gainidatzi, ezabatu eta agerian utz litzake. Era berean, DLLren bahiketa ahalbidetu lezake, bai eta pribilegioen igoera ere. Ahultasun horretarako CVE-2019-0381 identifikatzailea erabili da.

Gainerako ahultasunetarako honako identifikatzaileak esleitu dira: CVE-2019-0368, CVE-2019-0374, CVE-2019-0375, CVE-2019-0376, CVE-2019-0377, CVE-2019-0378, CVE-2019-0370, CVE-2019-0369, CVE-2019-0365 eta CVE-2019-0367.

Etiketak: Eguneraketa, SAP, Ahultasuna

Parametroen injekzio erako ahultasuna IBMren Spectrum Scale-n

Argitalpen data: 2019/10/09

Garrantzia: Altua

Kaltetutako baliabideak:

- BM Spectrum Scale:
  - 5.0.0.0 bertsiotik 5.0.3.2 bertsiora bitartekoak.
  - 4.2.0.0 bertsiotik 4.2.3.17 bertsiora bitartekoak.

Azalpena:

IBMek kritikotasun altuko ahultasun bat aurkitu du bere produktu batean. Erasotzaile batek *root* pribilegioak eskura litzake sisteman.

Konponbidea:

- 5.0.0.0tik 5.0.3.2ra bitarteko bertsioak dituzten produktuen kasuan, 5.0.3.3 bertsiora eguneratzea.
- 4.2.0.0tik 4.2.3.17ra bitarteko bertsioak dituzten produktuen kasuan, 4.2.3.18 bertsiora eguneratzea.

Xehetasuna:

Ahultasunaren jatorria da parametroen injekzioa setuid fitxategietan. Erasotzaile batek root pribilegioak eskura litzake sisteman. Ahultasun horretarako CVE-2019-4558 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Microsoften 2019ko urriko segurtasun buletina

Argitalpen data: 2019/10/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows,
- Internet Explorer,
- Microsoft Edge (EdgeHTML-based),
- ChakraCore,
- Microsoft Office, Microsoft Office Services eta Web Apps,
- SQL Server Management Studio,
- Open Source Software,
- Microsoft Dynamics 365,
- Windows Update Assistant.

Azalpena:

Segurtasun eguneraketen inguruko hileroko Microsoft-en argitalpenean 59 ahultasun jaso dira oraingoan; 10 kritiko gisa sailkatu dira eta 49 garrantzitsu gisa. Gainerakoak larritasun baxu edo ertainekoak dira.

Konponbidea:

Dagokion eguneraketa instalatzea. Segurtasun eguneraketen instalazioari buruzko informazio orrian eguneraketa metodo ezberdinei buruz informatzen da.

Xehetasuna:

Argitaratutako ahultasun motak honako hauek dira:

- zerbitzuaren ukapena,
- pribilegioen eskalatzea,
- informazioaren zabalkundea,
- kodearen urruneko exekuzioa,
- segurtasun ezaugarriaren gabezia,
- ordezpena,
- faltsutzea.

Etiketak: Eguneraketa, Adobe, Microsoft, Nabigatzailea, Ahultasuna, Windows

---

Kodearen urruneko exekuzioa SolarWinds-en Dameware Mini Remote Control-en

Argitalpen data: 2019/10/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Solarwinds Dameware Mini Remote Client Agent Service, 12.1.0.89 bertsioa.

Azalpena:

Tenablek larritasun kritikoko ahultasun bat aurkitu du. Autentifikaziorik gabeko urruneko erasotzaile batek gailuan kode arbitrarioa exekuta lezake.

Konponbidea:

Oraindik ez dago konponbiderik eskuragarri.

Xehetasuna:

SolarWinds Dameware Remote Mini Remote Client Agent Service-k bere modu lehenetsian txartel inteligenteen autentifikazioa onartzen du, eta horrela erabiltzaileak exekutagarri bat karga dezake DWRCS.exe *host*-ean. Exekutagarria C:*WindowsTemp*-en gordeko da *dwDrvInst.exe* izenarekin eta *Local System*-en kontuaren pribilegioekin exekutatuko da. Autentifikatu gabeko urruneko erasotzaile batek

txartel inteligentearen saioa hastea eska dezake fitxategi arbitrario bat kargatzeko eta exekutatzeko *Local System*-en kontuarekin. Ahultasun horretarako CVE-2019-3980 identifikatzailea erabili da.

Etiketak: Komunikazioak, Ahultasuna

Hainbat ahultasun Juniper produktuetan

Argitalpen data: 2019/10/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Junos OS 12.3X48, 15.1X49, 17.3, 17.4. Kaltetutako plataformak: SRX Series.
- Junos OS 18.1, 18.1X75, 18.2, 18.2X75, 18.3, 18.4. Kaltetutako plataformak: MX2008, MX2010, MX2020, MX480, MX960.
- Junos OS. Kaltetutako plataformak: NFX Series.
- Junos OS 12.3X48. Kaltetutako plataformak: SRX Series.
- Junos OS 18.1, 18.1X75.
- Junos OS 15.1X49, 18.2, 18.4. Kaltetutako plataformak: SRX Series.
- Junos OS 15.1X49, 15.1X53, 16.1, 16.2, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4.
- Junos OS 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 15.1X53, 16.1, 16.2, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1.
- Junos OS. Kaltetutako plataformak: SRX 5000 Series.
- Junos OS 16.1, 16.2, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4. Kaltetutako plataformak: MX Series.
- Junos OS 15.1, 15.1X49, 15.1X53, 16.1, 16.2, 17.1, 17.2, 17.3.
- Junos OS 12.1X46, 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 15.1X53, 16.1, 16.2, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4.
- Junos OS 15.1X49, 17.4, 18.1, 18.2, 18.3, 18.4. Kaltetutako plataformak: SRX1500.
- Junos OS 12.3X48, 15.1X49, 17.4, 18.1, 18.2, 18.3. Kaltetutako plataformak: SRX Series.
- Junos OS. Kaltetutako plataformak: NFX Series.
- Junos OS 18.1R3-S4, 18.3R1-S3.Kaltetutako plataformak: EX2300, EX2300-C, EX3400.
- Contrail Networking.

Azalpena:

Ohartarazpen honetan Junos OS eta Contrail Networking-ek dituzten hainbat ahultasunen berri ematen da.

Konponbidea:

Kaltetutako produktuak Juniper-en deskargen zentrotik eguneratzea.

Xehetasuna:

Asmo gaiztoko erabiltzaile batek Junos OSrako aipatutako ahultasunak baliatuko balitu, kaltetutako produktuetan honako ekintza hauek egin litzake:

- Zerbitzuaren ukapena: ahultasun horietarako CVE-2019-0055, CVE-2019-0056, CVE-2019-0059, CVE-2019-0060, CVE-2019-0064, CVE-2019-0065, CVE-2019-0066, CVE-2019-0050 eta CVE-2019-0075 identifikatzaileak erabili dira.
- Autentifikazioari ihes egitea: Ahultasun horretarako CVE-2019-0057 identifikatzailea erabili da.
- Pribilegioen eskalatzea: ahultasun horietarako CVE-2019-0058, CVE-2019-0061, CVE-2019-0070 eta CVE-2019-0071 identifikatzaileak erabili dira.
- Sarbidea lortzea administratzaile modura: ahultasun horretarako CVE-2019-0062 identifikatzailea erabili da.
- Junos gailuan administratzaile ekintzak egitea: ahultasun horretarako CVE-2019-0047 identifikatzailea erabili da.

Bestalde, Juniper Networks Contrail Networking-ek bere 1910 bertsioan erabiltzen duen hirugarrenen softwarearen hainbat ahultasun ere konpondu dira.Informazio gehiago eskuratzeko *Erreferentziak* atala irakurri.

Etiketak: Eguneraketa, Ahultasuna

XXE erako ahultasuna Dell EMCren hainbat produktutan

Argitalpen data: 2019/10/11

Garrantzia: Altua

Kaltetutako baliabideak:

- Dell EMC Avamar Server, 7.4.1, 7.5.0, 7.5.1, 18.2 eta 19.1 bertsioak;
- Dell EMC Integrated Data Protection Appliance (IDPA), 2.0, 2.1, 2.2, 2.3 eta 2.4 bertsioak.

Azalpena:

Dell EMCren hainbat produktuk larritasun altuko ahultasun bat daukate, Kanpoko XML Entitatearen (XXE) injekzio erakoa.

Konponbidea:

Dell-ek gomendatzen du *hotfix* ezberdinak aplikatzea, kaltetutako produktuen bertsioaren arabera:

- Dell EMC Avamar Server:
  - 7.4.1;
  - 7.5.0;
  - 7.5.1;
  - 18.2;
  - 19.1.
- Dell EMC Integrated Data Protection Appliance (IDPA):
  - 2.0;
  - 2.1;

- 2.2;
- 2.3;
- 2.4.

Xehetasuna:

XXE erako ahultasuna baliatuz autentifikatu gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake edo informazioa agerian utzi, dokumentuaren erako definizioak (DTD) ematean, bereziki diseinatutako XML eskaera batean. Ahultasun horretarako CVE-2019-3752 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Runas murrizpenen saihespena sudo-n

Argitalpen data: 2019/10/15

Garrantzia: Altua

Kaltetutako baliabideak:

Sudo, 1.8.28 bertsioa baino lehenagokoak.

Azalpena:

sudo-k duen kritikotasun altuko ahultasun bat baliatuz, erasotzaile batek *Runas* murrizpenak saihets litzake, eta komandoak exekutatu *root* modura.

Konponbidea:

1.8.28 bertsiora eguneratzea.

Xehetasuna:

sudo konfiguratzen denean erabiltzaileek *Runas*-en ALL parametroaren bitartez komando arbitrarioak exekutatu ahal izan ditzaten, posible da komandoak *root* modura exekutatzea -1 edo 4294967295 erabiltzaile IDak erabiliz. Autentifikatutako erabiltzaile lokal batek, *sudo* pribilegioak baditu, komandoak exekuta litzake sisteman *root* modura, *Runas*-en erabiltzaile murrizpenak saihestuz. Ahultasun horretarako CVE-2019-14287 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Linux, Ahultasuna

WordPress-entzat 5.2.4 segurtasun eguneraketa

Argitalpen data: 2019/10/15

Garrantzia: Ertaina

Kaltetutako baliabideak:

WordPress, 5.2.3 eta lehenagoko bertsioak.

Azalpena:

WordPress-en azken bertsioa argitaratu da, 6 segurtasun arazo zuzentzen dituena.

Konponbidea:

- 5.2.4 bertsiora eguneratzea.
- WordPress-en 5.1 eta lehenagoko bertsio eguneratuak ere eskuragarri daude 5.2 bertsiora eguneraketarik oraindik egin ez duen edozein erabiltzailerentzat.

Xehetasuna:

Segurtasun zuzenketek ondoko ahultasunak konpontzen dituzte, erasotzaile bati honakoa egitea ahalbidetuko lioketenak:

- Customizer-en bidez *Cross-Site Scripting* (XSS) erasoak egitea.
- autentifikatu gabeko mezuak ikustea.
- Javascript kodea injektatzea estilo etiketetan, Stored Cross-Site Scripting-en bidez.
- JSON GETen eskaeren cachea pozoitzea Vary-ren bidez.
- zerbitzariaren aldean eskaerak faltsutzea URLak baliozkotzen diren moduan.

Etiketak: Eguneraketa, CMS, Ahultasuna

Eguneraketa kritikoak Oracle-n (2019ko urria)

Argitalpen data: 2019/10/16

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Agile Recipe Management for Pharmaceuticals, 9.3.3 eta 9.3.4 bertsioak;
- Diagnostic Assistant, 2.12.36 bertsioa;
- Enterprise Manager Base Platform, 13.2 eta 13.3 bertsioak;

- Exadata-rako Enterprise Manager, 12.1.0.5.0, 13.2.2.0.0, 13.3.1.0.0 eta 13.3.2.0.0 bertsioak;
- Enterprise Manager Ops Center, 12.3.3 eta 12.4.0 bertsioak;
- Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2 eta M12-2S Servers, XCP2361 eta XCP3071 baino lehenagoko bertsioak;
- Hyperion Data Relationship Management, 11.1.2.4 bertsioa;
- Hyperion Enterprise Perparamance Management Architect, 11.1.2.4 bertsioa;
- Hyperion Financial Reporting, 11.1.2.4 bertsioa;
- Instantis EnterpriseTrack, 17.1, 17.2 eta 17.3 bertsioak;
- JD Edwards EnterpriseOne Tools, 4.0.1.0 bertsioa;
- MICROS Relate CRM Software, 7.1.0, 11.4, 15.0.0, 16.0.0, 17.0.0 eta 18.0.0 bertsioak;
- MICROS Retail XBRi Loss Prevention, 10.8.3 bertsioa;
- MySQL Connectors, 5.3.13 eta lehenagoko bertsioak, eta 8.0.17 eta lehenagokoak;
- MySQL Enterprise Monitor, 8.0.17 eta lehenagoko bertsioak;
- MySQL Server, 5.6.45 eta lehenagoko bertsioak, 5.7.27 eta lehenagokoak, 8.17 eta lehenagokoak;
- MySQL Workbench, 8.0.17 eta lehenagoko bertsioak;
- Oracle Agile PLM, 9.3.3-9.3.6 bertsioak;
- Oracle Agile Product Lifecycle Management for Process, 6.2.0.0, 6.2.1.0, 6.2.2.0, eta 6.2.3.0 bertsioak;
- Oracle API Gateway, 11.1.2.4.0 bertsioa;
- Oracle Application Testing Suite, 13.2 eta 13.3 bertsioak;
- Oracle Banking Digital Experience, 18.1, 18.2, 18.3 eta 19.1 bertsioak;
- Oracle Banking Platparam, 2.4.0, 2.4.1, 2.5.0, 2.6.0, 2.6.1, 2.7.0 eta 2.7.1 bertsioak;
- Oracle BI Publisher, 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak;
- Oracle Business Intelligence Enterprise Edition, 11.1.1.9.0, 12.2.1.3.0 eta 12.2.1.4.0 bertsioak;
- Oracle Clusterware, 19.0.0.0.0 bertsioa;
- Oracle Data Integrator, 12.2.1.3.0 bertsioa;
- Oracle Database Server, 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c eta 19c bertsioak;
- Oracle E-Business Suite, 12.1.1-12.1.3 eta 12.2.3-12.2.9 bertsioak;
- Oracle Enterprise Repository, 12.1.3.0.0 bertsioa;
- Oracle Financial Services Analytical Applications Infrastructure, 8.0.2-8.0.8 bertsioak;
- Oracle Financial Services Enterprise Financial Perparamance Analytics, 8.0.6 eta 8.0.7 bertsioak;
- Oracle Financial Services Retail Perparamance Analytics, 8.0.6 eta 8.0.7 bertsioak;
- Oracle FLEXCUBE Direct Banking, 12.0.2 eta 12.0.3 bertsioak;
- Oracle params, 12.2.1.3.0 bertsioa;
- Oracle GoldenGate Application Adapters, 12.3.2.1.0 bertsioa;
- Oracle GraalVM Enterprise Edition, 19.2.0 bertsioa;
- Oracle Healthcare Foundation, 7.1.1 eta 7.2.2 bertsioak;
- Oracle Healthcare Translational Research, 3.1.0, 3.2.1 eta 3.3.1 bertsioak;
- Oracle Hospitality Cruise Dining Room Management, 8.0.80 bertsioa;
- Oracle Hospitality Guest Access, 4.2.0 eta 4.2.1 bertsioak;
- Oracle Hospitality Materials Control, 18.1 bertsioa;
- Oracle Hospitality Reporting and Analytics, 9.1.0 bertsioa;
- Oracle Hospitality RES 3700, 5.7 bertsioa;
- Oracle Java SE, 7u231, 8u221, 11.0.4 eta 13 bertsioak;
- Oracle Java SE Embedded, 8u221 bertsioa;
- Oracle JDeveloper eta ADF, 11.1.1.9.0, 11.1.2.4.0, 12.1.3.0.0 eta 12.2.1.3.0 bertsioak;
- Oracle NoSQL Database, 19.3.12 baino lehenagoko bertsioak;
- Oracle Outside In Technology, 8.5.4 bertsioa;
- Oracle Policy Automation, 10.4.7, 12.1.0, 12.1.1 eta 12.2.0-12.2.15 bertsioak;
- Oracle Policy Automation Connector for Siebel, 10.4.6 bertsioa;
- Oracle Policy Automation for Mobile Devices, 12.2.0-12.2.15 bertsioak;
- Oracle Retail Customer Insights, 15.0 eta 16.0 bertsioak;
- Oracle Retail Customer Management eta Segmentation Foundation, 17.x bertsioa;
- Oracle Retail Integration Bus, 15.0 eta 16.0 bertsioak;
- Oracle Retail Xstore Office, 7.1 bertsioa;
- Oracle Retail Xstore Point of Service, 7.1, 15.0, 16.0, 17.0, 17.0.3, 18.0, 18.0.1 eta 19.0.0 bertsioak;
- Oracle Service Bus, 11.1.1.9.0, 12.1.3.0.0 eta 12.2.1.3.0 bertsioak;
- Oracle SOA Suite, 12.2.1.3.0 bertsioa;
- Oracle Solaris, 10 eta 11 bertsioak;
- Oracle Virtual Directory, 11.1.1.9.0 bertsioa;
- Oracle VM VirtualBox, 5.2.34 baino lehenagoko bertsioak eta 6.0.14 baino lehenagokoak;
- Oracle Web Services, 12.2.1.3.0 bertsioa;
- Oracle WebCenter Portal, 12.2.1.3.0 bertsioa;
- Oracle WebLogic Server, 10.3.6.0.0, 12.1.3.0.0 eta 12.2.1.3.0 bertsioak;
- PeopleSoft Enterprise HCM Human Resources, 9.2 bertsioa;
- PeopleSoft Enterprise PeopleTools, 8.56 eta 8.57 bertsioak;
- PeopleSoft Enterprise SCM eProcurement, 9.2 bertsioa;
- Primavera Gateway, 15.2, 16.2, 17.12 eta 18.8 bertsioak;
- Primavera P6 Enterprise Project Portfolio Management, 15.1.0-15.2.18, 16.1.0-16.2.18, 17.1.0-17.12.14 eta 18.1.0-18.8.13 bertsioak;
- Primavera Unifier, 16.1, 16.2, 17.7-17.12 eta 18.8 bertsioak;
- Siebel Applications, 19.8 eta lehenagoko bertsioak.

Azalpena:

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

Konponbidea:

Kaltetutako produktuen arabera, dagozkien partxeak aplikatzea. Eguneraketak deskargatzeko informazioa Oraclek argitaratutako segurtasun buletinean lor daiteke.

Xehetasuna:

Eguneraketa horrek 219 ahultasun konpontzen ditu guztira, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna *Erreferentziak* atalean dagoen Oracleren loturan kontsulta daiteke.

Etiketak: Eguneraketa, Java, Oracle, Birtualizazioa, Ahultasuna

---

Ahultasuna IBMren Workload Scheduler-en

Argitalpen data: 2019/10/16

Garrantzia: Altua

Kaltetutako baliabideak:

- Tivoli Workload Scheduler Distributed, 9.2.0 FP03 eta lehenagoko bertsioak.
- IBM Workload Scheduler Distributed:
  - 9.3.0 FP03 eta lehenagoko bertsioak,
  - 9.4.0 FP05 eta lehenagoko bertsioak,
  - 9.5.0 GA bertsioa.

Azalpena:

Davide Cioccia-k, INGko segurtasun ingeniari seniorra, kritikotasun altuko ahultasuna aurkitu du. Erasotzaile lokal batek fitxategiak alda litzake edo *root* pribilegioak eskuratu sisteman.

Konponbidea:

IBMk eguneraketak argitaratu ditu, kaltetutako bertsio, produktu eta plataformen arabera. Bere softwarearen deskarga zentroan eskura daitezke.

Xehetasuna:

Ahultasunaren jatorria da erabiltzaile lokal batek fitxategiak idatzi ahal izatea *root* modura fitxategien sisteman. Erasotzaile lokal batek fitxategiak alda litzake edo *root* pribilegioak eskuratu sisteman. Ahultasun horretarako CVE-2019-4031 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Sarbidearen kontrol desegokia VMware produktuetan

Argitalpen data: 2019/10/16

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- VMware Cloud Foundation,
- PCFrako VMware Harbor Container Registry, 1.8.X bertsioak.

Azalpena:

Aipatutako VMware produktuetan sarbidearen kontrol desegoki erako ahultasun bat aurkitu da PCF helbide hautsietan.

Konponbidea:

- VMware Cloud Foundation-en kasuan, ahultasuna konpontzen duen partxea laster argitaratuko da.
- PCFrako VMware Harbor Container Registry-ren kasuan, 1.8.4 partxea aplikatu behar da.

Xehetasuna:

Sarbide hautsiaren kontrol erako ahultasun bat baliatuz, proiektu batera administratzaile sarbidea lukeen erasotzaile batek alboko proiektu baten barnean robot kontu bat sor lezake Harbor-en APIaren bidez. Horren ondorioz baimenik gabeko sarbide bat gerta liteke, xede den alboko proiektuan irudiak txertatu, atera edo aldatzeko. Ahultasun horretarako CVE-2019-16919 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/10/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Ondokoen bertsio ahul bat exekutatzen ari diren Cisco produktuak:
  - Aironet 1540 Series APs,
  - Aironet 1560 Series APs,
  - Aironet 1800 Series APs,
  - Aironet 1810 Series APs,
  - Aironet 1830 Series APs,
  - Aironet 1850 Series APs,
  - Aironet 2800 Series APs,
  - Aironet 3800 Series APs,
  - Aironet 4800 APs,
  - Catalyst 9100 APs (8.9.100.0 bertsioa da zerbitzua duen lehena).
- Cisco WLC Software, 8.5.140.0 eta lehenagoko bertsioak;
- Cisco SPA112 2-Port Phone Adapter eta SPA122 ATA Router-duna, *firmware*-aren 1.4.1 SR4 bertsioa eta lehenagokoak, webean oinarritutako kudeaketa interfazea gaituta duenean;
- Cisco 250 Series Smart Switches;
- Cisco 350 Series Managed Switches;
- Cisco 550X Series Stackable Managed Switches.

Azalpena:

Ciscok bere produktuei eragiten dieten 18 ahultasunen berri eman du, bat larritasun kritikokoa eta 17 larritasun altukoak.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Cisco Software-ren deskarga paneletik deskarga daitezke.

Xehetasuna:

Erasotzaile batek ohartarazpen honetan azaldutako ahultasunen bat balia lezake honako ekintza hauetakoren bat egin ahal izateko:

- gailura baimenik gabeko sarbidea pribilegio altuekin;
- zerbitzuaren urruneko ukapena;
- kodearen urruneko exekuzioa;
- urrunetik CSRF (*Cross-Site Request Forgery*) erasoen exekuzioa.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Autentifikazio okerra ABBren hainbat gailutan

Argitalpen data: 2019/10/18

Garrantzia: Txikia

Kaltetutako baliabideak:

- UNO-DM, 1.8.2 bertsioa eta lehenagokoak;
- PVS-100-TL eta PVS120-TL, 0.10.14 bertsioa eta lehenagokoak;
- PVS-175-TL, 0.2.6 bertsioa eta lehenagokoak;
- PVS-50/60 eta TRIO-TM, 1.2.15 bertsioa eta lehenagokoak;
- REACT 2, 0.2.19 bertsioa eta lehenagokoak.

Azalpena:

Maxim Rupp ikertzaileak autentifikazio oker erako ahultasun baten berri eman du. Hori baliatuz erasotzaile batek kaltetutako produktuen informaziora sarbidea lor lezake autentifikatu behar izan gabe.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- UNO-DM 1.8.3 bertsioa.
- PVS-100-TL eta PVS120-TL 0.10.15 bertsioa.
- PVS-175-TL, 0.2.7 bertsioa.
- PVS-50/60 eta TRIO-TM, 1.2.16 bertsioa.
- REACT 2, 0.2.20 bertsioa.

Xehetasuna:

Autentifikazio oker erako ahultasuna baliatuz, produktuak zenbait informaziora irakurketa moduan sarbidea izatea lor liteke, aldez aurretik autentifikazio prozesu bat egin behar izan gabe. Ahultasun horretarako ez da identifikatzailerik esleitu.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioak eskalatzearen erako ahultasuna Fortinet-en FortiMail-en

Argitalpen data: 2019/10/21

Garrantzia: Altua

Kaltetutako baliabideak:

- FortiMail, honako bertsioak:
  - 6.2.0,
  - 6.0.0tik 6.0.6ra bitartekoak,
  - 5.4.10 eta lehenagokoak.

Azalpena:

Fortinet-ek kritikotasun altuko bi ahultasun aurkitu ditu FortiMail-en. Administratzaile pribilegioak lituzkeen erasotzaile batek sistemara baimenik gabeko sarbidea lor lezake.

Konponbidea:

- FortiMail-en honako bertsioetara eguneratzea:
  - 6.2.1,
  - 6.0.7,
  - 5.4.11 (oraindik argitaratzeko).

Xehetasuna:

- Bi ahultasunak administrazioko web erabiltzailearen interfazean aurkitzen dira, eta horrela administratzaileek baimenik gabeko ekintzak egin litzakete:
  - Administratzaile pribilegioak lituzkeen erasotzaile batek web kontsolara baimenik gabeko sarbidea lor lezake. Ahultasun horretarako CVE-2019-15712 identifikatzailea erreserbatu da.
  - Administratzaile pribilegioak lituzkeen erasotzaile batek baimenik gabeko sarbidea lor lezake eta sistemaren segurtasun kopiaren konfigurazioa deskargatu. Ahultasun horretarako CVE-2019-15707 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Autentifikazioa saihestea Citrix Application Delivery Controller eta Citrix Gateway-en

Argitalpen data: 2019/10/21

Garrantzia: Altua

Kaltetutako baliabideak:

- Citrix ADC eta Citrix Gateway 13.0 bertsioa, build 41.20 bitartekoak;
- Citrix ADC eta NetScaler Gateway 12.1 bertsioa, build 54.13 bitartekoak;
- Citrix ADC eta NetScaler Gateway 12.0 bertsioa, build 62.8 bitartekoak;
- Citrix ADC eta NetScaler Gateway 11.1 bertsioa, build 62.8 bitartekoak;
- Citrix ADC eta NetScaler Gateway 10.5 bertsioa, build 70.5 bitartekoak.

Azalpena:

Ahultasun bat aurkitu da Citrix Application Delivery Controller-en (ADC) kudeaketa interfazean, aurretik NetScaler ADC modura ezaguna, eta Citrix Gateway-enean, aurretik NetScaler Gateway modura ezaguna.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- Citrix ADC and Citrix Gateway 13.0 bertsioaren kasuan, build 41.28 eta ondorengoak;
- Citrix ADC and Citrix Gateway 12.1 bertsioaren kasuan, build 54.16 eta ondorengoak;
- Citrix ADC and Citrix Gateway 12.0 bertsioaren kasuan, build 62.10 eta ondorengoak;
- Citrix ADC and Citrix Gateway 11.1 bertsioaren kasuan, build 63.9 eta ondorengoak;
- Citrix ADC and Citrix Gateway 10.5 bertsioaren kasuan, build 70.8 eta ondorengoak.

Xehetasuna:

Kaltetutako produktuek administrazio interfazean duten ahultasun bat baliatuz, erasotzaile batek horretara sarbidea balu, gailura sartzea lor lezake administratzaile baimenekin.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna IBMren Security Access Manager-en

Argitalpen data: 2019/10/25

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Security Access Manager-en bertsio guztiak.

Azalpena:

Lczap segurtasun ikertzaileak kritikotasun altuko ahultasun baten berri eman dio IBMri. Autentifikatu gabeko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake.

Konponbidea:

Oraingoz ez dago ahultasun hori konpontzen duen eguneraketarik. Eraso mota hauek arintzeko IBMk argibide batzuk argitaratu ditu.

Xehetasuna:

IBM Security Access Manager ahula da Slow HTTP Attack erako erasoen aurrean. Autentifikatu gabeko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake sisteman. Ahultasun horretarako CVE-2019-4036 identifikatzailea erreserbatu da.

Etiketak: IBM, Ahultasuna

Hainbat ahultasun MikroTik-en RouterOS-en

Argitalpen data: 2019/10/29

Garrantzia: Altua

Kaltetutako baliabideak:

- RouterOS Stable, 6.45.6 eta lehenagoko bertsiodunak,
- RouterOS Long-term, 6.44.5 eta lehenagoko bertsiodunak.

Azalpena:

Tenable-ko segurtasun ikertzailea den Jacob Baines-ek kritikotasun altuko 4 ahultasun aurkitu ditu. Autentifikaziorik gabeko urruneko erasotzaile batek gailura sarbidea lortu, hura aldatu edo *root* pribilegioak eskura litzake.

Konponbidea:

- MikroTik ahultasunak konpontzen dituzten eguneraketak argitaratu ditu:

- RouterOS Stable, 6.45.7 bertsiora eguneratzea,
- RouterOS Long-term, 6.44.6 bertsiora eguneratzea.

Xehetasuna:

- Ahultasunetako baten jatorria da 8291 atakari DNS eskaerak egin ahal izatea.Autentifikatu gabeko urruneko erasotzaile batek DNS cachearen pozoitze erako eraso bat egin lezake gailuan. Ahultasun horretarako CVE-2019-3978 identifikatzailea erabili da.
- Ahultasunetako baten jatorria DNS erantzunen maneiu desegokia da. Urruneko erasotzaile batek, kaltetutako DNS zerbitzari baten bidez, asmo gaiztoko eskaerak bidal litzake router-aren DNS cache-a pozoitzeko. Ahultasun horretarako CVE-2019-3979 identifikatzailea erabili da.
- Ahultasunetako baten jatorria eguneraketen paketeen izenaren eremua da. Erasotzaile batek asmo gaiztoko eguneraketa pakete bat sor lezake, eta hori erabiltzaile autentifikatu batek gailuan instalatuz gero, terminal bat gaitu lezake *root* pribilegioekin. Ahultasun horretarako CVE-2019-3976 identifikatzailea erabili da.
- Ahultasunetako baten jatorria eguneraketen paketeen baliozkotze eza da, autoeguneraketen parametroa aktibo dagoenean. Urruneko erasotzaile batek router-aren *firmwarearen downgrade* bat egin lezake, eta erabiltzaileak eta pasahitzak berrabiatu. Ahultasun horretarako CVE-2019-3977 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Zerbitzuaren ukapena RDesktop-en

Argitalpen data: 2019/10/31

Garrantzia: Altua

Kaltetutako baliabideak:

RDesktop, 1.8.4 bertsioa baino lehenagokoak.

Azalpena:

Kaspersky ICS CERTeko Pavel Cheremushkin segurtasun ikertzaileak RDesktop-en ahultasun bat aurkitu du. Hori baliatuz urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake.

Konponbidea:

1.8.5 bertsiora eguneratzea.

Xehetasuna:

Mugaz kanpoko irakurketa erako hainbat ahultasun baliatuz, erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake.

Etiketak: Eguneraketa, Ahultasuna