2020ko Ekainaren Bulletina

Ohartarazpenak - Teknikoak

Datuen prozesatzearen akatsen ahultasuna Cisco produktuetan

Argitalpen data: 2020/06/02

Garrantzia: Altua

Kaltetutako baliabideak:

Ahultasun horrek Cisco produktu hauei eragiten die, Cisco NX-OS softwarearen bertsio ahul bat exekutatzen ari badira:

- Nexus 1000 Virtual Edge para VMware vSphere;
- Nexus 1000V Switch para Microsoft Hyper-V y VMware vSphere;
- Nexus 3000, 6000 y 7000 Series Switches;
- Nexus 9000 Series Switches en modo independiente NX-OS;
- Nexus 5500 y 5600 Platform Switches;
- UCS 6200 y 6300 Series Fabric Interconnects.

Azalpena:

Yannay Livneh ikertzaileak kritikotasun handiko ahultasun bat atzeman du hainbat Cisco produktutan. Datuen prozesatze akatsen motakoa da.

Konponbidea:

Abisuaren Fixed Software atalean zehaztutako ahultasuna konpontzen duten eguneratzeak Cisco Software panelean deskargatu daitezke:

Xehetasuna:

Cisco NX-OS softwarearen sareko ahultasun honen ondorioz, egiaztatu gabeko urrutiko erasotzaile batek kaltetutako gailuan segurtasun muga batzuk saltatu litzake, edo zerbitzuaren ukapen baldintza bat sortu. Ahultasun horretarako, CVE-2020-10136 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Arubaren ClearPass Policy Manager sistemako ahultasunak

Argitalpen data: 2020/06/03

Garrantzia: Altua

Kaltetutako baliabideak:

- Clear Pass Policy Manager 6.9.x, 6.9.1 bertsioaren aurrekoak;
- Clear Pass Policy Manager 6.8.x, 6.8.5-HF bertsioaren aurrekoak;
- Clear Pass Policy Manager 6.7.x, 6.7.13-HF bertsioaren aurrekoak;

Azalpena:

Daniel Jensen ikertzaileak hiru ahultasunen berri eman zion Arubari; bi kritikotasun handikoak eta beste bi tartekoak. Motak: kodea urrutitik exekutatzea eta egiazkotasuna saihestea.

Konponbidea:

- Clear Pass Policy Manager 6.9.x 6.9.1 bertsiora eguneratzea;
- Clear Pass Policy Manager 6.8.x bertsioa 6.8.5-HF edo 6.8.6 bertsiora eguneratzea;
- Clear Pass Policy Manager 6.7.x bertsioa 6.7.13-HF bertsiora eguneratzea;

Xehetasuna:

- Webgunearen interfazeak egiaztatze-ihesaren arloko ahultasun bat dauka. Urrutiko erasotzaile batek, ahultasun hori baliatuta, azpiko sistema eragilea atzitu lezake. Ahultasun horretarako, CVE-2020-7115 identifikatzailea erreserbatu da.
- Administrazioko web interfazeak bi ahultasun ditu; bata handia eta beste bestea tartekoa, kodea urrutitik exekutatzeari dagozkionak. Aurretik interfazean egiaztatutako erasotzaile batek kodearen urrutiko exekuzioa burutu lezake azpiko sistema eragilean. Ahultasun horietarako CVE-2020-7116 eta CVE-2020-7117 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Segurtasun-eguneratzea: Joomla! 3.9.19

Argitalpen data: 2020/06/03

Garrantzia: Ertaina

Kaltetutako baliabideak:

- Joomla! CMS, honako bertsioak:
  - 2.5.0tik 3.9.18ra;
  - 3.0.0tik 3.9.18ra.

Azalpena:

Joomla! Sistemak bertsio berri bat argitaratu du. Bere guneari eragiten dioten 5 ahultasun konpontzen ditu. Kritikotasun ertaineko ahultasun bat eta kritikotasun baxuko lau konpontzen ditu. Motak: *Cross-site scripting* (XSS), *Cross-site request forgery* (CSRF) eta berezko konfigurazioetan akatsak gertatzea.

Konponbidea:

Joomla! 3.9.19 bertsiora eguneratzea.

Xehetasunak:

- Tarteko kritikotasunak jQuery-ren DOM-aren manipulazio metodoei eragiten die, eta XSS eraso bat gerta liteke. Ahultasun horietarako CVE-2020-11022 eta CVE-2020-11023 identifikatzaileak erreserbatu dira.
- Larritasun baxuko ahultasunak ondoren azalduta daude:
-
  - "Articles ? Newsflash" y "Articles ? Categories" moduluen etiketen goiburuetako aukeran sartzeko parametroak ez balioztatuta, XSS erasoak gerta litezke. Ahultasun horretarako, CVE-2020-13761 identifikatzailea esleitu da.
  - "Textfilter" konfigurazio globalaren berezko parametroek ez dute gonbidatutako erabiltzaileen HTML sarrerarik blokeatzen ("Guest"). CVE-2020-13763 kodea esleitu zaio ahultasun horri.
  - Com_modules moduluaren etiketa aukeran sartzeko balioztatzea oker eginda, XSS erasoak gerta litezke. Ahultasun horretarako, CVE-2020-13762 identifikatzailea esleitu da.
  - com_postinstall sisteman tokenak ez konprobatzeak CSRF motako eraso bat bideratu lezake. Ahultasun horretarako CVE-2020-13760 identifikatzailea esleitu da.

Etiketak: Eguneraketa, CMS, Ahultasuna

SO komandoen injekzio arloko ahultasuna IBM Security Guardium sisteman

Argitalpen data: 2020/06/03

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Security Guardium, 11.1 bertsioa.

Azalpena:

IBM Security Guardium sistemaren ahultasun hori baliatuz, erasotzaile batek komando arbitrarioak exekutatu litzake sisteman.

Konponbidea:

Ahultasuna konpontzen duen partxea aplikatzea.

Xehetasuna:

Ahultasun horren bidez, urrutitik egiaztatutako erasotzaile batek komando arbitrarioak exekutatu litzake sisteman, bereziki diseinatutako eskaera baten bidez. Ahultasun horretarako, CVE-2020-4180 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

XXE Injekzio ahultasuna IBM QRadar sisteman

Argitalpen data: 2020/06/04

Garrantzia: Altua

Kaltetutako baliabideak:

SDEE protokoloaren hauen aurreko bertsio guztiak (*Security Device Event Exchange*):

- 7.3.0-QRADAR-PROTOCOL-SDEE-7.3-20200429181957;
- 7.4.0-QRADAR-PROTOCOL-SDEE-7.4-20200429181942

Azalpena:

IBM X-Force Ethical Hacking Team taldeko hainbat kidek larritasun handiko ahultasun bat atzeman dute, XXE injekzio motakoa (*XML External Entity*). IBMren QRadar produktuari eragiten dio.

Konponbidea:

Kaltetutako produktua honako bertsioetara eguneratzea: 7.4.0-QRADAR-PROTOCOL-SDEE-7.4-20200429181942 edo 7.3.0-QRADAR-PROTOCOL-SDEE-7.3-20200429181957.

Xehetasuna:

IBM QRadar sistema XML External Entity (XXE) injekzio eraso baten eraginpean egon daiteke, XML datuak prozesatzean. Urrutiko erasotzaile batek ahultasun hori baliatu lezake informazio konfidentziala agerian utzi edo memoriaren baliabideak kontsumitzeko. Ahultasun horretarako, CVE-2020-4509 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Egiaztatze-ihesaren motako ahultasuna GnuTLS inplementazioan

Argitalpen data: 2020/06/04

Garrantzia: Altua

Kaltetutako baliabideak:

GnuTLS, 3.6.4 bertsioa.

Azalpena:

Ahultasun bat atzeman GnuTLS inplementazioaren TLS zerbitzarian. Horrela, erasotzaile batek TLS 1.3 egiaztatzea saihestu ahal izango luke, eta TLS 1.2 bertsioan aurreko elkarrizketak berreskuratu.

Konponbidea:

3.6.14 edo osteko bertsioen arabera eguneratzea.

Xehetasuna:

GnuTLS inplementazioaren zerbitzariak gai dira horietako bakoitzak jaulkitako tiketak erabiltzeko, *gnutls_session_ticket_key_generate()* sistemak sortutako gako sekretuaren beharrik gabe. Horrela izanik, MITM erasotzaile batek, egiaztatzeko datu baliagarririk gabe, aurretik datu zuzenekin hasitako konexio bateko saioak berreskuratu litzake. Ahultasun horretarako, CVE-2020-13777 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioa, Ahultasuna

Hainbat ahultasun atzeman dira Cisco-ren gailuetan

Argitalpen data: 2020/06/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco IOS XE, 16.3.1 bertsioa eta aurrekoak, IOS XE hosting infrastructure aplikazioa konfiguratuta izanez gero.
- Cisco IOS Software sistemaren bertsio ahul bat exekutatzen ari diren honako produktuak:
  - Cisco 809 and 829 Industrial ISRs,
  - CGR1000,
- Cisco IOS;
- Cisco IOS XE;
- Cisco IOS XXR;
- Cisco IOS XE, UI webgunea gaituta;
- Cisco IOS XE, HTTP zerbitzari ezaugarria gaituta;
- Cisco IOS edo Cisco IOS XE, CIP-erako konfiguratuta. CIP ez dator berez konfiguratuta;
- Cisco IOS edo Cisco IOS XE, SSH konexioak onartzeko konfiguratuta;
- Cisco IOS edo Cisco IOS XE, IKEv2 ezaugarria konfiguratuta. IKEv1 ezaugarria duten gailuek ez dute kalterik jasan.
- Cisco Catalyst Series Switches, Cisco IOS edo Cisco IOS XE sistemen bertsio ahul bat exekutatzen badute:
  - Cisco Catalyst 4500, SNMP polling-erako konfiguratuta, Power over Ethernet (PoE) txartelak instalatuta;
  - Aplication Visibility and Control (AVC) ezaugarria gaituta duten edo LSCekin konfiguratuta dauden Cisco Catalyst 9800.
  - Catalyst 3650 Series Switches;
  - Catalyst 3850 Series Switches;
  - Catalyst 9200 Series Switches;

    - Catalyst 9300 Series Switches;
    - Catalyst 9500 Series Switches.
- Cisco IOS edo Cisco IOS XSren bertsio ahulak exekutatzen dituzten Routers Cisco tresnak, honako ezaugarriak konfiguratuta:
    - Cisco Unified Border Element (CUBE);
    - Cisco Unified Communications Manager Express (CME);
    - Cisco IOS Gateways con Session Initiation Protocol (SIP)
    - Cisco TDM Gateways;
    - Cisco Unified Survivable Remote Site Telephony (SRST);
    - Cisco Business Edition 4000 (BE4K).
- Cisco NX-OS daukaten eta onePK ezaugarria gaituta duten honako gailuak:
    - Nexus 3000 Series Switches;
    - Nexus 5500 Platform Switches;
    - Nexus 5600 Platform Switches;
    - Nexus 6000 Series Switches;
    - Nexus 7000 Series Switches;
    - Nexus 9000 Series Switches en modo NX-OS independiente (*standalone*).
- 1.9.0 bertsioaren aurreko IOx Application Framework sistemaren bertsioak exekutatzen dituzten gailuak:
    - 800 Series Industrial Integrated Services Routers (Industrial ISRs);
    - 800 Series Integrated Services Routers (ISRs);
    - 1000 Series Connected Grid Routers (CGR1000) Compute Module;
    - IC3000 Industrial Compute Gateway;
    - Industrial Ethernet (IE) 4000 Series Switches;
    - IOS XE sistemetan oinarritutako gailuak:
        - 1000 Series ISRs,
        - 4000 Series ISRs,
        - ASR 1000 Series Aggregation Services Routers,
        - Catalyst 9x00 Series Switches,
        - Catalyst IE3400 Rugged Series Switches,
        - Embedded Services 3300 Series Switches,
    - IR510 WPAN Industrial Routers.

Azalpena:

Ciscok hainbat produkturi eragiten dieten 26 ahultasun atzeman ditu, 4 kritikoak eta 22 larritasun handikoak.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneratzeak Ciscoren Softwarearen deskarga paneletik deskargatu daitezke: Informazio zehatzagoa izateko, kontsultatu Erreferentzien atala.

Xehetasuna:

Atzemandako ahultasunen ondorioz, erasotzaile batek honako ekintzak burutu litzake:

- Pribilegioak handitzea,
- Komandoen injekzioa,
- Kode arbitrarioa exekutatzea,
- Root pribilegioak dituen urrutiko kode exekuzioa,
- Zerbitzua ukatzeko baldintza sortzea (DoS),
- Gailuan baimendu gabeko softwarea instalatzea,
- Kredentzial barneratuen bidez sisteman sartzea,
- Fitxategiak manipulatzea.

Larritasun kritikoko ahultasunei honako identifikatzaileak esleitu zaizkie: CVE-2020-3227, CVE-2020-3205, CVE-2020-3198 eta CVE-2020-3198.

Etiketak: Eguneraketa, CISCO, Ahultasuna

SSRF ahultasuna IBM Maximo Asset Management sisteman

Argitalpen data: 2020/06/08

Garrantzia: Altua

Kaltetutako baliabideak:

- IBM Maximo Asset Management, 7.6.0 eta 7.6.1 bertsioak;
- Industria konponbideen arloko produktu kaltetuak, bertsio nagusi kaltetu bat erabiliz gero:
    - iAbiaziorako Maximo,
    - Bizi-zientzietarako Maximo,
    - Energia nuklearrerako Maximo,
    - Petrolio eta gaserako Maximo,
    - Garraiorako Maximo,
    - Zerbitzu publikoetarako Maximo;
- Kaltetutako IBM Control Desk produktuak, bertsio nagusi kalteturen bat erabiltzen badute:
    - SmartCloud Control Desk,
    - IBM Control Desk,
    - Tivoli Integration Composer.

Azalpena:

Postive Technologies enpresako Andrey Medov eta Arseniy Sharoglazov ikertzaileek larritasun handiko ahultasun baten berri eman dioten IBM erakundeari, SSRF motakoa (Server Side Request Forgery). Fabrikatzailearen Maximo Asset Management produktuari eragiten dio.

Konponbidea:

IBM Maximo Asset Management sistemaren 7.6.0.4 bertsiotik, *applet* gabeko inprimaketa funtzioa gehitu zen, eta *applet* inprimaketa desaktibatuta dago, mugarik gabe. Ahultasun hori konpontzeko, applet inprimaketaren erabilera saihestu behar da.

Xehetasuna:

Ahultasun horren bidez, erasotzaile egiaztatu batek baimendu gabeko eskaerak bidal litzake sistematik, eta horrek sarearen enumerazioa eragin lezake (erabiltzaileen, gailu multzoen eta ordenagailu sare batekin erlazionatutako bestelako zerbitzuekin erlazionatutako informazioa lortzea) edo beste eraso batzuk bideratu. Ahultasun horretarako, CVE-2020-4529 identifikatzailea erreserbatu da.

Etiketak: IBM, Ahultasuna

Ahultasuna UPnP-ren inplementazioan

Argitalpen data: 2020/06/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Protocolo Universal Plug and Play (UPnP), 2020ko apirilaren 17aren aurreko bertsioa.

Azalpena:

Yunus Çadirci ikertzaileak ahultasun baten berri eman du Universal Plug and Play protokoloan (UPnP). Trafiko bidalketa xede arbitrarioetara bideratu daiteke SUBSCRIBE funtzionaltasuna erabiliz.

Konponbidea:

- OCF erakundeak UPnP zehaztapena eguneratu du arazo hori konpontzeko. Erabiltzaileek saltzaileen euskarriak monitorizatu behar dituzte, azken horiek SUBSCRIBE zehaztapen berria ezarri bitartean.
- Gailu fabrikatzaileei eskatu zaie SUBSCRIBE gaitasuna desgaitzeko aurrez ezarritako konfigurazioan, eta erabiltzaileei eskatzeko funtzio hori gaitu dezatela sareko muga egokiekin, erabilera konfiantzazko tokiko sare batera mugatzeko.
- Hurrengo Suricata IDS arauak kanpo sare baterako edozein HTTP SUBSCRIBE eskaera bilatzen du, hau da, ez RFC1918 edo RFC4193 helbideak. Sareko administrari eta Interneteko zerbitzuen hornitzaileek sinadura hori hedatu dezakete Interneterako sarbide-puntuan, erabiltzaileei heltzen zaien edozein SUBSCRIBE eskaera bitxi atzemateko.
-
    - alert http any any - > ![fd00::/8,192.168.0.0/16,10.0.0.0/8,172.16.0.0/12] any (msg:"UPnP SUBSCRIBE request seen to external network VU#339275: CVE- 2020-12695 https://kb.cert.org "; content: "subscribe"; nocase; http_met hod; sid:1367339275;)

Xehetasuna:

UPnP SUBSCRIBE gaitasunaren ahultasun baten ondorioz, urrutiko erasotzaile batek datu-kopuru handiak bidal litzake helmuga irisgarrietara Internet bidez. Hori dela eta, zerbitzu ukapen banatua gerta liteke (DDoS), datuen exfiltrazioa eta bestelako ustekabeko portaera batzuk. Ahultasun horretarako CVE-2020-12695 identifikatzailea esleitu da. Call Stranger ere deitzen zaio.

Etiketak: Komunikaziak, Ahultasuna

Hainbat ahultasun Liferay Portal sisteman

Argitalpen data: 2020/06/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Liferay Portal, vhonako bersioak:

- 7.2.1 eta aurrekoak;
- 7.x, 7.3.2 aurrekoak;
- 7.1.3, 7.2.0, 7.2.1 eta ziur aski aurreko ez bateragarriak.

Azalpena:

Hainbat ikertzailek ahultasun batzuk atzeman dituzte Liferay Portal edukien kudeatzailean; larritasun kritikoko 4 (fabrikatzaileek severity 1 gisa sailkatua), eta larritasun altu eta ertaineko 11 (severity 2 gisa sailkatua Liferay-k erabilitako baremoaren arabera). Ahultasun motak honakoak dira: Deserializazioa Javan, LDAP kredentzialak agerian geratzea, REST datuen hornitzailearen pasahitza galtzea, kodearen urrutiko exekuzioa, CSRF, SSRF, XSS, MitM, artxiboen luzapenaren mugari ihes egitea, direktorioetarako sarbidea kontrolik gabe, postaren injekzioa, erabiltzaileen baimenen konprobazio falta eta instantzia egin daitekeen widget baten instantzia ez konfiguratua.

Konponbidea:

Honako bertsioetara eguneratzea:

- Liferay Portal 7.2 GA2 (7.2.1),
- Liferay Portal 7.1 GA4 (7.1.3),
- Ez dago partxerik Liferay Portal 7.3.1 bertsiorako eta aurrekoetarako. 7.3 CE GA3 (7.3.2) edo ostekoak erabili behar dira zuzenean;
- Ez dago partxerik Liferay Portal 7.2.0 bertsiorako. 7.2 CE GA2 (7.2.1) edo ostekoak erabili behar dira zuzenean;

Xehetasuna:

Erasotzaile batek honako ekintzak burutu litzake, aurretik aipatutako ahultasunen bat baliatuz gero:

- Jakinarazpenak ikusi eta aldatzea;
- LDAP kredentzialak lortzea;
- Urrutiko erabiltzaile egiaztatu batek REST Data Providers-eko pasahitza lortu lezake. Ahultasun horretarako, CVE-2020-13444 identifikatzailea erreserbatu da.
- Urrutiko erabiltzaile egiaztatu batek kode arbitrarioa exekutatu lezake bereziki diseinatutako txantiloien bidez. Ahultasun horretarako, CVE-2020-13445 identifikatzailea erreserbatu da.
- Informazio sentikorra ikustea;

- Urrutiko erasotzaile batek script web arbitrarioa edo HTML injektatu lezake;
- Sisteman artxiboak gainidaztea;
- Phishing erasoa;
- Erabiltzailea kanpo webgune batera birbideratzea;
- Urrutiko erabiltzaile egiaztatuek webguneko erabiltzaile-taldeak kontsultatu litzakete, webgunearen beraren administrazio panelaren bidez.

Etiketak: Eguneraketa, CMS, Ahultasuna

Microsoften segurtasun buletina. 2020ko ekaina

Argitalpen data: 2020/06/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows;
- Microsoft Edge (EdgeHTML sisteman oinarritua);
- Microsoft Edge (Chromium sisteman oinarritua) IE moduan;
- Microsoft ChakraCore;
- Internet Explorer;
- Microsoft Office, Microsoft Office Services y Web Apps;
- Windows Defender;
- Microsoft Dynamics;
- Visual Studio;
- Azure DevOps;
- HoloLens;
- Adobe Flash Player;
- Microsoft Apps para Android;
- Windows App Store;
- System Center;
- Android App.

Azalpena:

Segurtasun eguneratzeen inguruko hileroko Microsoft argitalpenean 129 ahultasun jaso dira oraingoan; 11 kritiko gisa sailkatu dira eta 118 garrantzitsu gisa.

Konponbidea:

Dagokion segurtasun-eguneratzea instalatzea. Microsoften orrian eguneratze horiek egiteko azalpenak eman dira.

Xehetasuna:

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Kodearen urrutiko exekuzioa.
- Pribilegioak handitzea,
- Zerbitzua ukatzea.
- Informazioa zabaltzea.
- Nortasuna ordeztea (spoofing),
- Segurtasun-mugei ihes egitea.

Etiketak: Eguneratzea, Microsoft, Nabigatzailea, Ahultasuna, Windows

---

Ahultasunak TIBCO konpainiaren IBM i sistemarako Managed File Transfer Platform Server zerbitzarian

Argitalpen data: 2020/06/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

IBM i-rako TIBCO Managed File Transfer Platform Server, bertsioak:

- 7.1.0 eta aurrekoak;
- 8.0.0.

Azalpena:

TIBCO konpainiak larritasun kritikoko bi ahultasun argitaratu ditu. Komandoen exekuzio arbitrario, informazioa argitaratze eta fitxategien baimendu gabeko manipulazio arlokoak dira.

Konponbidea:

IBM i-rako TIBCO Managed File Transfer Platform Server honako bertsioetara eguneratzea:

- 7.11 edo hortik gorakoak;
- 8.0.1 edo hortik gorakoak.

Xehetasuna:

File transfer osagaiari eragiten dioten ahultasun kritikoak ondoren azaltzen dira:

- Egiaztatu gabeko urrutiko erasotzaile batek komando arbitrarioak exekutatu litzake kaltetutako sistemaren pribilegioekin, transferentzia akastun baten ondoren. Ahultasun horretarako, CVE-2020-9412 identifikatzailea esleitu da.
- Require Node Resp konfigurazio-aukera Ez aukeran konfiguratuta dagoenean. Urrutiko erasotzaile batek, egiaztatu gabe, sistemaren artxiboak eskuratu eta manipulatu litzake, eta horrek gailuaren sistema eragilearen integritatean eragin lezake. Ahultasun horretarako, CVE-2020-9411 identifikatzailea esleitu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Intel erakundearen segurtasun buletina. 2020ko ekaina

Argitalpen data: 2020/06/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Intel Converged Security and Manageability Engine (CSME);
- Intel Server Platform Services (SPS);
- Intel Trusted Execution Engine (TXE);
- Intel Active Management Technology (AMT);
- Intel Standard Manageability (ISM);
- Intel Dynamic Application Loader (DAL);
- Intel SSD, serieak:
  - D3-S4510;
  - DC P4510;
  - DC P4610;
  - DC P4618;
  - DC P4511;
  - D5-P4326;
  - D5-P4420;
  - D5-P4320.
- Intelen prozesatzaile batzuk; ondoko zerrendan kontsulta daitezke:
- Intel Core prozesagailu familien BIOS tresnen firmwarea:
-
  - 7. Belaunaldia;
  - 8. Belaunaldia;
  - 9. Belaunaldia;
  - 10. Belaunaldia.
- Intel Innovation Engine Build eta Signing Tool, 1.0.859. bertsioaren aurrekoak.

Intel produktuetan atzemandako ahultasunek honako fabrikatzaileei eragiten diete:

- Citrix/Xen:
  - Citrix Hypervisor 8.0;
  - Citrix Hypervisor 8.1;
  - XenServer 7.0;
  - XenServer 7.1 LTSR Cumulative Update 2.

Azalpena:

Hainbat ikertzaile eta erakundek 25 ahultasunen berri eman diote Intel erakundeari. Horietatik, 2 larritasun kritikokoak dira, 11 altukoak, 11 ertainekoak eta bat baxukoa.

Konponbidea:

Intelek eguneratze batzuk argitaratu ditu; ahultasunak produktuaren eta kaltetutako bertsioen arabera konpontzen dituzte: Informazio zehatzago izateko, joan *Erreferentzien atalera*.

Ahultasun horien eragina jaso duten fabrikatzaileentzako:

- Citrix / Xen:
  - Citrix Hypervisor 8.1, CTX272278 partxea;
  - Citrix Hypervisor 8.0, CTX272277 partxea;
  - Citrix XenServer 7.1 LTSR CU2, CTX272276 partxea
  - Citrix XenServer 7.0, CTX272275 partxea.

Xehetasuna:

Atzemandako ahultasunen ondorioz, erasotzaile batek honako ekintzak burutu litzake:

- Pribilegioak handitzea,
- Zerbitzua ukatzeko baldintza sortzea,
- Informazioa argitara ematea.

CVE-2020-0543 identifikatzailea duen ahultasuna nabarmentzea, CROSSTALK izenekoa. Erasotzaile batek informazioa argitara eman lezake.

Larritasun kritikoko ahultasunei CVE-2020-0594 eta CVE-2020-0595 identifikatzaileak erreserbatu zaizkie.

Kritikotasun maila altuko ahultasunei honako identifikatzaileak erreserbatu zaizkie: CVE-2020-0586, CVE-2020-0542, CVE-2020-0596, CVE-2020-0538, CVE-2020-0534, CVE-2020-0533, CVE-2020-0532, CVE-2020-0566, CVE-2020-0527, CVE-2020-0528 eta CVE-2020-8675.

Etiketak: Eguneraketa, Ahultasuna

2020ko ekaineko SAP segurtasunaren eguneratzea

Argitalpen data: 2020/06/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Liquidity Management for Banking, 6.2 bertsioa;
- SAP Commerce, 6.7, 1808, 1811 eta 1905 bertsioak;
- SAP Commerce (Data Hub), 6.7, 1808, 1811 eta 1905 bertsioak;
- SAP Commerce, 6.7, 1808, 1811 eta 1905 bertsioak;
- SAP Solution Manager (Problem Context Manager), 7.2 bertsioa;
- SAP SuccessFactors Recruiting, 2005 bertsioa;
- SAP Netweaver AS ABAP, 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753 eta 754 bertsioak;
- SAP NetWeaver AS JAVA (P4 Protocol), bertsioak:
  - SAP-JEECOR 7.00 eta 7.01;
  - SERVERCOR 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50;
  - CORE-TOOLS 7.00, 7.01, 7.02, 7.05, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50;
- SAP NetWeaver AS ABAP (Banking Services), 710, 711, 740, 750, 751, 752, 75A, 75B, 75C, 75D eta 75E bertsioak;
- SAP Solution Manager (Trace Analysis), 7.20 bertsioa;
- Adobe LiveCycle Designer, 11.0 bertsioa;
- SAP NetWeaver AS ABAP (Business Server Pages Test Application SBSPEXT_TABLE), 700, 701, 702, 730, 731, 740, 750, 751, 752, 753 eta 754 bertsioak;
- SAP Fiori for SAP S/4HANA, 200, 300, 400 eta 500 bertsioak;
- SAP ERP (Statutory Reporting for Insurance Companies), EA-FINSERV 600, 603, 604, 605, 606, 616, 617, 618 eta 800, eta S4CORE 101, 102, 103 eta 104 bertsioak;
- SAP Business One(Backup service), 9.3 eta 10.0 bertsioak;
- SAP Gateway, 7.40, 2.00, 7.5, 7.51, 7.52 eta 7.53 bertsioak;
- SAP Business Objects Business Intelligence Platform, 4.2 bertsioa.

Azalpena:

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

Konponbidea:

- SAPen laguntzarako ataria bisitatu eta eguneratze edo partxeak instalatzea, fabrikatzaileak adierazitakoaren arabera.
- CVE-2020-6265 ahultasunerako emandako partxeak SAP Commerce (Data Hub) instalazio berriei soilik eragiten die, ez ditu dauden instalazioetan sartutako kontuetako pasahitz aurrez ezarriak kentzen, beraz, fabrikatzaileak proposatzen du partxea aplikatu ostean SAP Commerce instalazioa berrabiaraztea.
- CVE-2020-1938 ahultasunerako, Ghostcat izeneko Apache Tomcat-eko ahultasun ezagun baten ondorioz, SAP-ek biziki gomendatzen du Apache JServ protokoloa erabiltzen duten portu guztiak desaktibatzea (AJP protokoloa). Bezeroek protokolo hori behar izatekotan, AJP konektorearen konfigurazioan eskatzen den atributu sekretua ezartzea gomendatzen da.

Xehetasuna:

SAPek 17 segurtasun ohar eta eguneratze 1 egin ditu bere hileroko jakinarazpenean. Horietako 2 larritasun kritikokoak dira, 4 altukoak eta 12 tartekoak.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:s:

- Cross-site scripting delakoaren ahultasun bat.
- Kredentzial barneratuen ahultasun bat.
- Informazioaren dibulgazioaren arloko 3 ahultasun.
- Egiaztatze faltaren arloko ahultasun bat,
- Egiaztatzea konprobatzeko faltaren 3 ahultasun,
- XML balioztatze faltako 3 ahultasun,
- URL helbideko 2 ahultasun,
- Beste motaren bateko 6 ahultasun.

Beste motaren bateko 6 ahultasun.:

- SAP Commerce and SAP Commerce Data Hub produktuek erabiltzaile kontu batzuk erabiltzen dituzte; pasahitzak publikoki ezagunak dira eta administrariek ez dute pasahitz horiek aldatzeko betebeharrik aplikazioa instalatu bitartean edo ostean. Ahultasun horretarako, CVE-2020-6265 identifikatzailea erreserbatu da.
- AJP konexioak ustiatzeko, urrutiko erasotzaile batek kode exekuzioa eta bestelako eragiketa batzuk baimendu litzake. Ahultasun horretarako, CVE-2020-1938 identifikatzailea esleitu da.
- Propietate batzuen konfigurazio espezifikoarekin, erasotzaile batek ezaugarri ez seguruak ustiatu litzake saioa hasteko formularioan, eta lortutako informazioa beste exploit eta eraso batzuetarako erabil liteke etorkizunean. Propietate horietako batzuk berez konfiguratuta daude. Ahultasun horretarako CVE-2020-6264 kodea erreserbatu da.

Etiketak: Eguneraketa, SAP, Ahultasuna

Pribilegioen eskalatzea VMware Horizon Client-en

Argitalpen data: 2020/06/11

Garrantzia: Altua

Kaltetutako baliabideak:

Windowserako VMware Horizon Client, 5.4.3 baino lehenagoko bertsioak.

Azalpena:

Windowserako VMware Horizon Client-ek duen pribilegioen eskalatze erako ahultasun bat argitaratu da.

Konponbidea:

5.4.3 bertsiora eguneratzea.

Xehetasuna:

Windowserako VMware Horizon Client-ek pribilegioen eskalatze erako ahultasun bat dauka, karpetaren baimenen konfigurazioaren eta liburutegien karga ez-seguruaren ondorioz. Ahultasun horretarako CVE-2020-3961 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Segurtasun eguneratzea 5.4.2 WordPress-erako

Argitalpen data: 2020/06/11

Garrantzia: Handia

Kaltetutako baliabideak:

WordPress, 5.4.1 bertsioa eta aurrekoak.

Azalpena:

WordPress-en azken bertsioa argitaratu da, eta 6 segurtasun arazo konpondu dira horren bidez.

Konponbidea:

5.4.2 bertsiora eguneratzea.

Xehetasuna:

Segurtasun-zuzenketek konpontzen dituzten ahultasunen ondorioz, erasotzaileak honako aukerak izan litzake:

- XSS egitea (Cross-Site Scripting),
- Birbideratze irekia: wp_validate_redirect(),
- Pribilegioen eskalatzea set-screen-option sistemaren erabilera okerraren bidez.
- Baldintza zehatz batzuen arabera babestutako iruzkin eta pasahitzak erakustea.

Etiketak: Eguneratzea, CMS, Ahultasuna

Hainbat ahultasun Paloalto produktuetan

Argitalpen data: 2020/06/11

Garrantzia: Altua

Kaltetutako baliabideak:

- PAN-OS:
  - 9.0.7-ren aurreko 9.0 bertsioak;
  - 8.1.13-ren aurreko 8.1 bertsioak;
  - 8.0 bertsio guztiak.
  - 7.1 bertsio guztiak.
- GlobalProtect App:
  - 5.1.4 bertsioaren aurreko windowserako 5.1. bertsioak
  - 5.0.10 bertsioaren aurreko windowserako 5.0. bertsioak

Azalpena:

Paloalto produktuen hainbat ahultasun argitaratu dira. Horien bidez, erasotzaile batek sistemaren prozesuak eten litzake, eta root pribilegioak dituen kode arbitrarioa exekutatu, sistema eragileko komandoak exekutatu root pribilegioekin, edo SYSTEM pribilegioekin programak exekutatu.

Konponbidea:

Eguneratzea:

- PAN-OS:
  - 9.0.7 bertsioa;
  - 8.1.13 bertsioa;
  - 8.0 bertsioak euskarri amaieran daude eta ez dute eguneratzerik izango;
  - 7.1 bertsioak ahultasun kritikoetarako soilik eguneratuko dira;
- GlobalProtect App:
  - 5.1.4 bertsioak edo hortik gorakoak;
  - 5.0.10 bertsioak edo hortik gorakoak;

Xehetasuna:

- PAN-OS kudeaketa zerbitzariaren authd osagaiko buferraren gainezkatze motako ahultasun baten ondorioz, egiaztatutako administrariek sistemaren prozesuak eten litzakete eta kode arbitrarioa exekutatu root pribilegioekin. Ahultasun horretarako, CVE-2020-2027 identifikatzailea esleitu da.
- PAN-OS administrazio zerbitzariaren sistema eragilearen komandoen injekzioko ahultasun baten ondorioz, administrari egiaztatuek sistema eragileko komando arbitrarioak exekutatu litzakete root pribilegioekin, FIPS-CC motako ziurtagiri berri bat igota. Ahultasun horretarako, CVE-2020-2028 identifikatzailea esleitu da.
- PAN-OS sistemaren web administrazioaren interfazean sistema eragilearen komandoen injekzioko ahultasun bat egotearen ondorioz, administrari egiaztatuek komando arbitrarioak exekutatu litzakete root pribilegioekin, eta eskaera maltzur bat bidali PAN-OS konfigurazioan erabiltzeko ziurtagiri berriak sortzeko. Ahultasun horretarako, CVE-2020-2029 identifikatzailea esleitu da.
- GlobalProtect, Windowseko karrera izaerako ahultasun baten ondorioz, tokiko erabiltzaile batek programak exekutatu litzake SYSTEM pribilegioekin. Arazo hori ustiatzeko, GlobalProtect aplikazioaren eguneratze bat egin behar da. Ahultasun horretarako, CVE-2020-2032 identifikatzailea esleitu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Citrix-en zenbait produktutan

Argitalpen data: 2020/06/12

Garrantzia: Altua

Kaltetutako baliabideak:

- Windowserako Citrix Receiver, bertsio guztiak;
- Citrix Workspace App, 1912 baino lehenagoko bertsioak.

Azalpena:

Andrew Hess ikertzaileak bi ahultasun aurkitu ditu, biak larritasun altukoak, lehenetsitako baimen oker erakoak.

Konponbidea:

Kaltetutako bi produktuen erabiltzaileak Citrix Workspace App eguneratu behar dute 1912 edo geroagoko bertsioetara, LTSR bertsioetan jasoak.

Xehetasuna:

Kaltetutako produktuen desinstalazio prozesuan erabiltzaile lokal batek pribilegioak eskala litzake administratzaile izatera iritsi arte. Ahultasun horietarako CVE-2020-13884 eta CVE-2020-13885 identifikatzaileak erabili dira.

Etiketak: Eguneraketa, Birtualizazioa, Ahultasuna

Hainbat ahultasun IBM produktuetan

Argitalpen data: 2020/06/15

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Spectrum Protect Plus, 10.1.0 bertsiotik 10.1.5 bertsiora bitartekoak.

Azalpena:

Hainbat ahultasun aurkitu dira IBM produktuetan. Horiek baliatuz erasotzaile batek kodearen urruneko exekuzioa egin lezake, zerbitzuaren ukapena eragin, autentifikazioa saihestu edo DNS saioak bahitu.

Konponbidea:

IBM Spectrum Protect Plus-en 10.1.6 bertsiora eguneratzea.

Xehetasuna:

- IBM Spectrum Protect Plus baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake sisteman, bereziki diseinatutako HTTP komando bat erabiliz. Ahultasun horretarako CVE-2020-4469 identifikatzailea erabili da.
- IBM Spectrum Protect Plus baliatuz autentifikatu gabeko erasotzaile batek zerbitzuaren ukapena eragin lezake edo DNS saioak bahitu, bereziki diseinatutako HTTP komando bat bidaliz urruneko zerbitzarira. Ahultasun horretarako CVE-2020-4471 identifikatzailea erreserbatu da.
- IBM Spectrum Protect Plus-en Administrazio Kontsola baliatuz, autentifikatutako erasotzaile batek fitxategi arbitrarioak igo litzake zerbitzari ahulean kode arbitrarioa exekutatzeko. Ahultasun horretarako CVE-2020-4470 identifikatzailea erreserbatu da.
- IBM Spectrum Protect Plus-ek kodetutako kredentzialak ditu, esate baterako pasahitz edo gako kriptografiko bat, bere sarrera autentifikazio propiorako, kanpo osagaietarako irteera komunikaziorako eta barne datuak zifratzeko erabiltzen dituena. Ahultasun horretarako CVE-2020-4216 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Netgear-en produktuetan

Argitalpen data: 2020/06/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Ondoko produktuak, horietan 3.2.15.25 baino lehenagoko firmware bertsioak exekutatzen direnean:

- RBK752,
- RBK753,
- RBK753S,
- RBR750,
- RBS750,
- RBK852,
- RBK853,
- RBR850,
- RBS850,
- RBK842,

- RBR840,
- RBS840.

Azalpena:

Netgear-ek bere produktuei eragiten dieten 15 ahultasunen berri eman du, 12 larritasun kritikokoak eta 3 larritasun altukoak.

Konponbidea:

Netgear-en zerbitzu orrialdera sartzea eta kaltetutako gailuaren azken firmware bertsioa deskargatzea.

Xehetasuna:

Netgear-ek argitaratutako ohar multzoan deskribatutako ahultasun motak honako hauek dira:

- administratzaile kredentzialak zabaltzea,
- komandoen injekzioa autentifikazioaren ondoren,
- komandoen injekzioa autentifikazioaren aurretik,
- CSRF (Cross Site Request Forgery).

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun Ciscoren produktuetan

Argitalpen data: 2020/06/18

Garrantzia: Altua

Kaltetutako baliabideak:

- Cisco Webex Meetings, honako bertsioak:
  - WBS 39.5.25 eta lehenagokoak;
  - WBS 40.4.10 eta lehenagokoak;
  - WBS 40.6.0.
- Cisco Webex Meetings Server, 4.0MR3 eta lehenagoko bertsioak;
- Cisco Webex Meetings Desktop App, 39.5.12 baino lehenagoko bertsioak;
- Mac-erako Cisco Webex Meetings Desktop App, 39.5.11 baino lehenagoko bertsioak;
- Cisco TelePresence Collaboration Endpoint Software eta RoomOS Software, May Drop 2 2020 baino lehenagoko bertsioak;
- Cisco Small Business, router eta firmware bertsio hauek:
-
  - RV016 Multi-WAN VPN 4.2.3.10 eta lehenagokoak;
  - RV042 Dual WAN VPN 4.2.3.10 eta lehenagokoak;
  - RV042G Dual Gigabit WAN VPN 4.2.3.10 eta lehenagokoak;
  - RV082 Dual WAN VPN 4.2.3.10 eta lehenagokoak;
  - RV320 Dual Gigabit WAN VPN 1.5.1.05 eta lehenagokoak;
  - RV325 Dual Gigabit WAN VPN 1.5.1.05 eta lehenagokoak;
  - RV110W Wireless-N VPN Firewall 1.2.2.5 eta lehenagokoaks;
  - RV130 VPN Router 1.0.3.54 eta lehenagokoak;
  - RV130W Wireless-N Multifunction VPN Router 1.0.3.54 eta lehenagokoak;
  - RV215W Wireless-N VPN Router 1.3.1.5 eta lehenagokoak.

Azalpena:

Ciscok hainbat produkturi eragiten dieten larritasun altuko 23 ahultasun aurkitu ditu.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Software de Ciscoren deskarga paneletik deskarga daitezke. Informazio zehatzagoa eskuratzeko Erreferentziak atala irakurri.

Xehetasuna:

Aurkitutako ahultasunak baliatuz urruneko erasotzaile batek ondoko ekintzak egin litzake:

- baimenik gabeko sarbidea lortzea Webex webgune ahul batera,
- programak exekutatzea azken erabiltzailearen sisteman,
- kode arbitrarioa exekutatzea,
- fitxategien sistema aldatzea zerbitzuaren ukapen egoera (DoS) sortzeko edo fitxategien sisteman root pribilegioak eskuratzeko.

Honako identifikatzaile hauek esleitu dira: CVE-2020-3361, CVE-2020-3263, CVE-2020-3342, CVE-2020-3336, CVE-2020-3286, CVE-2020-3287, CVE-2020-3288, CVE-2020-3289, CVE-2020-3290, CVE-2020-3291, CVE-2020-3292, CVE-2020-3293, CVE-2020-3294, CVE-2020-3295, CVE-2020-3296, CVE-2020-3268, CVE-2020-3269, CVE-2020-3274, CVE-2020-3275, CVE-2020-3276, CVE-2020-3277, CVE-2020-3278 eta CVE-2020-3279.

Etiketak: Ahultasuna, Cisco, Eguneraketa

Ahultasuna Drupal-en corean

Argitalpen data: 2020/06/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Honakoak baino lehenagoko bertsioak:

- 9.0.1;
- 8.9.1;

- 8.8.8;
- 7.72.

Azalpena:

Segurtasun eguneraketa berri bat argitaratu da, Drupal-en nukleoak dituen hiru ahultasun konpontzen dituena.

Konponbidea:

7.72, 8.8.8, 8.9.1 edo 9.0.1 bertsioetara eguneratzea.

Xehetasunak:

- Drupal-en corearen inprimakien APIak ez ditu modu egokian erabiltzen cross-site erako eskaeren inprimakien sarrera batzuk, eta horrek beste ahultasun batzuk eragin ditzake. Ahultasun horretarako CVE-2020-13663 identifikatzailea erreserbatu da.
- Drupal 8n eta 9n baldintza batzuetan gertatzen den urruneko kodearen exekuzio erako ahultasun bat baliatuz, erasotzaile batek administratzaile bat engaina lezake asmo gaiztoko webgune bat bisita dezan, eta horren ondorioz fitxategien sisteman kontu handiz izendatutako direktorio bat sor liteke. Direktorio hori bere lekuan izanda, erasotzaile bat urruneko kodearen exekuzio erako ahultasun bat eragiten saia liteke. Windows zerbitzariak dira kaltetuenak. Ahultasun horretarako CVE-2020-13664 identifikatzailea erreserbatu da.
- JSON:API PATCH eskaerek eremu batzuetako baliozkotzeak saihets ditzakete. Bere modu lehenetsian, JSON:APIk soilik funtzionatzen du irakurketa moduan, eta horrek ezinezkoa egiten du ahultasuna baliatzea. jsonapi.settings-en read-only aukera FALSE modura konfiguratuta duten webguneak soilik dira ahulak. Ahultasun horretarako CVE-2020-13665 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun Dell IMCren zenbait produktutan

Argitalpen data: 2020/06/19

Garrantzia: Handia

Kaltetutako baliabideak

- Dell EMC Isilon OneFS, 8.2.2 eta lehenagoko bertsioak;
- Dell EMC PowerScale OneFS, 9.0.0 bertsioa;
- PowerMax-erako Dell EMC Unisphere, 9.1.0.17 baino lehenagoko bertsioak;
- PowerMax Virtual Appliance-rako Dell EMC Unisphere, 9.1.0.17 baino lehenagoko bertsioak;
- PowerMax OS Release 5978.

Azalpena:

Dell-ek hiru ahultasunen berri eman du, horietatik bi Karlsruhe Institute of Technology-ko Thorsten Tüllmann-ek aurkituak. Bi larritasun altukoak dira eta bat ertainekoa, baimenen esleipen oker, ziurtagiriaren baliozkotze oker eta autentifikazioaren saihespen erakoak.

Konponbidea:

- Dell EMC Isilon OneFS eta Dell EMC PowerScale OneFS-ren kasuan, /ifs-n baimenak aldatu ondoren zehazten den moduan:

```
chmod 755 /ifs
chmod  a group admin allow generic_write,delete_child,std_write_dac /ifs
chmod  a user compadmin allow generic_write,delete_child,std_write_dac /ifs
```

- PowerMax-erako Dell EMC Unisphere-ren kasuan: 9.1.0.17 edo bertsio berriagoetara eguneratzea;
- PowerMax Virtual Appliance-rako Dell EMC Unisphere-ren kasuan: 9.1.0.17 edo bertsio berriagoetara eguneratzea;
- PowerMax OS Release 5978.221.221 edo 5978.479.479ren kasuan: fabrikatzailea arazoa konpontzeko ePack bat prestatzen ari da.

Xehetasuna:

- Sareko fitxategietara edo lokaletara sarbidea lukeen erasotzaile batek modu ez-nahikoan ezarritako fitxategi baimenak balia litzake fitxategi horietara baimendu gabeko sarbidea lortzeko, horrela sistema kaltetua arriskuan jarriz. Ahultasun horretarako CVE-2020-5371 identifikatzailea erreserbatu da.
- Autentifikatu gabeko urruneko erasotzaile batek man-in-the-middle erako eraso bat egin lezake bereziki diseinatutako ziurtagiri bat emanez, eta erabiltzailearen trafikoa atzemanez ibilbidean dauden bere datuak ikusi edo aldatzeko. Ahultasun horretarako CVE-2020-5367 identifikatzailea erreserbatu da.

Larritasun ertaineko ahultasunerako CVE-2020-5345 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Zerbitzuaren ukapen erako ahultasunak Squid-en

Argitalpen data: 2020/06/22

Garrantzia: Handia

Kaltetutako baliabideak:

Squid-en ondoko bertsioei bi ahultasunek eragiten diete:

- 3.1 bertsiotik 3.5.28 bertsiora bitartekoak;
- 4.0 bertsiotik 4.11 bertsiora bitartekoak;
- 5.0.1 bertsiotik 5.0.2 bertsiora bitartekoak.

Azalpena:

Bloomberg-eko Jack Zar eta Open Systems-eko Christof Gerber eta Mario Galli ikertzaileek bi ahultasun aurkitu dituzte, biak larritasun

altukoak, zerbitzuaren ukapen (DoS) erakoak.

Konponbidea:

- CVE-2020-14059 ahultasunaren kasuan, 5.0.3 bertsiora eguneratzea edo Squid 5-erako partxea aplikatzea;
- CVE-2020-14058 ahultasunaren kasuan, 4.12 edo 5.0.3 bertsioetara eguneratzea, edo Squid 4 edo Squid 5-erako partxeak aplikatzea.

Xehetasuna:

- Sinkronizazio oker baten ondorioz, Squid ahula da zerbitzuaren ukapen erako (DoS) eraso baten aurrean SMP cache batean objektuak prozesatzean. Arazo hori baliatuz urruneko bezero batek Squid-en worker baten asertzio bat aktiba lezake. Ahultasun horretarako CVE-2020-14059 identifikatzailea erreserbatu da.
- Arriskutsua izan litekeen funtzio bat erabiltzearen ondorioz, Squid eta ziurtagiriak egiaztatzeko lehenetsitako morroia ahulak dira zerbitzuaren ukapen erako (DoS) eraso baten aurrean TLS ziurtagiriak prozesatzean. Ahultasun horretarako CVE-2020-14058 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun VMware produktuetan

Argitalpen data: 2020/06/25

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- VMware ESXi, 7.0, 6.7 eta 6.5 bertsioak;
- VMware Workstation Pro / Player (Workstation), 15.x bertsioak;
- VMware Fusion Pro / Fusion (Fusion), 11.x bertsioak;
- VMware Cloud Foundation, 4.x eta 3.x bertsioak.

Azalpena:

VMware ESXi, Workstation eta Fusion-ek dituzten hainbat ahultasunen berri eman du VMware-k. Guztira 10 ahultasunen berri eman dute, 1 kritikoa, 5 altuak eta 4 ertainak.

Konponbidea:

Kaltetutako produktuetarako azken partxeak instalatzea gomendatzen da, erabilitako bertsio egonkorraren arabera:

- VMware ESXi: ESXi_7.0.0-1.20.16321839, edo ESXi670-202004101-SG, edo ESXi650-202005401-SG.
- VMware Workstation Pro / Player (Workstation): 15.5.5.
- VMware Fusion Pro / Fusion (Fusion): 11.5.5.
- VMware Cloud Foundation: 4.0.1 (oraindik argitaratzeko), edo 3.10 edo 3.10.0.1 (oraindik argitaratzeko).

Xehetasuna:

VMware-k ezagutzera emandako ahultasunen artetik kritikoena baliatuz, 3D grafikoak gaituta dituen makina birtual batera sarbide lokala lukeen erasotzaile batek kodea exekuta lezake hiperbisorean makina birtualetik bertatik, SVGA gailu batean askatu ondoreneko memoria erabiltzen duen 'use-after-free' erako ahultasun baten bidez. Ahultasun horretarako CVE-2020-3962 identifikatzailea erabili da.

Gainerako ahultasunetarako identifikatzaile hauek esleitu dira: CVE-2020-3963, CVE-2020-3964, CVE-2020-3965, CVE-2020-3966, CVE-2020-3967, CVE-2020-3968, CVE-2020-3969, CVE-2020-3970 eta CVE-2020-3971.

Etiketak: Eguneraketa, Birtualizazioa, VMware, Ahultasuna

Hainbat ahultasun Dell EMC produktuetan

Argitalpen data: 2020/06/25

Garrantzia: Handia

Kaltetutako baliabideak:

- Dell EMC Avamar Server, hardware appliance Gen4S, 7.4 eta ondorengo bertsioak, SUSE Linux Enterprise 11SP1-en;
- Dell EMC Avamar Server, hardware appliance Gen4T, 7.4 eta ondorengo bertsioak, SUSE Linux Enterprise 11SP3-n;
- Dell EMC Avamar Server, hardware appliance Gen4S/Gen4T, 7.4 eta ondorengo bertsioak, SUSE Linux Enterprise 11SP4-en;
- Dell EMC Avamar Server, hardware appliance Gen4S/Gen4T, 19.2 eta ondorengo bertsioak, SUSE Linux Enterprise 12SP4-en;
- Dell EMC Avamar Server, hardware appliance Gen4S/Gen4T, 19.3 eta ondorengo bertsioak, SUSE Linux Enterprise 12SP5-en;
- Dell EMC Avamar Virtual Edition, 7.4 eta ondorengo bertsioak, SUSE Linux Enterprise 11SP3-n;
- Dell EMC Avamar Virtual Edition, 7.4 eta ondorengo bertsioak, SUSE Linux Enterprise 11SP4-n (Azure eta AWS deployments barne 7.5.1 bertsiotik aurrera);
- Dell EMC Avamar Virtual Edition, 19.2 bertsioak, SUSE Linux Enterprise 12SP4-n (Azure eta AWS deployments barne);
- Dell EMC Avamar Virtual Edition, 19.3 bertsioak, SUSE Linux Enterprise 12SP5-en (Azure eta AWS deployments barne);
- Dell EMC Avamar NDMP Accelerator, 7.4 eta ondorengo bertsioak, SUSE Linux Enterprise 11SP1, SP3 eta 12SP4-n;
- Dell EMC Avamar VMware Image Proxy, 7.4 eta ondorengo bertsioak, SUSE Linux Enterprise 11SP1 edo SUSE Linux Enterprise 11SP3-n;
- Dell EMC Avamar VMware Image Proxy, 7.5.1 eta ondorengo bertsioak, SUSE Linux Enterprise 12SP1 edo SUSE Linux Enterprise 11SP4-n;
- Dell EMC NetWoker Virtual Edition (NVE), 18.x eta ondorengo bertsioak, SUSE Linux Enterprise 11SP3 edo SP4-n;
- Dell EMC vCloud Directo Data Protection Extension, 2.0.6 eta ondorengo bertsioak, SUSE Linux Enterprise 11SP3-n;
- Dell EMC Integrated Data Protection Appliance (IDPA), 2.0, 2.1, 2.2, 2.3, 2.4 eta 2.5 bertsioak;
- Dell Power Protect DataManager (PPDM), 19.4 baino lehenagoko bertsioak;
- Dell Power Protect X400, 3.2 baino lehenagoko bertsioak.

Azalpena:

Dell EMC Avamar eta NetWorker-en osagaiei eragiten dieten ahultasunetarako hainbat konponbide argitaratu dira, bai eta Dell Power Protect Data Manager-en beste ahultasun baterako ere, erasotzaile bati kaltetutako sistema arriskuan jartzea ahalbidetuko liokeena.

Konponbidea:

Honako eguneraketak aplikatzea:

- SLES11 SP1/SP3/SP4, SLES12 SP4/SP5 Avamar: AvPlatformOsRollup_2020-R2-v6.avp;
- SLES11 SP3/SP4 NVE: NvePlatformOsRollup_2020-R2-v6.avp;
- Avamar Proxy Bundle 2020-R2-v6;
- Dell Power Protect Data Manager 19.4 bertsioa;
- Dell Power Protect X400 3.2 bertsioa.

Xehetasuna:

- Dell Power Protect Data Manager (PPDM) eta Dell Power Protect X400-ek duten baimentze desegoki erako ahultasun bat baliatuz, urrunetik autentifikatutako erasotzaile batek edozein fitxategi deskarga lezake kaltetutako Power Protect-en makina birtualetatik. Ahultasun horretarako CVE-2020-5356 identifikatzailea erreserbatu da.
- Dell EMC Avamar eta NetWorker barneko hainbat osagaik segurtasun eguneraketa bat behar dute ahultasun horiei aurre egin ahal izateko.

Etiketak: Eguneraketa, Ahultasuna

HTTP/2-ko zerbitzuaren ukapenak Apache Tomcat-en hainbat bertsiori eragiten die

Argitalpen data: 2020/06/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Apache Tomcat, honako bertsioak:

- 8.5.0 bertsiotik 8.5.55 bertsiora bitartekoak;
- 9.0.0.M1 bertsiotik 9.0.35 bertsiora bitartekoak;
- 10.0.0-M1 bertsiotik 10.0.0-M5 bertsiora bitartekoak.

Azalpena:

Apache Tomcat-en 8, 9 eta 10 bertsioek zerbitzuaren ukapen (DoS) erako ahultasun bat daukate, HTTP/2 protokoloari eragiten diona.

Konponbidea:

Honako bertsioetara eguneratzea:

- 8.5.56;
- 9.0.36;
- 10.0.0-M6.

Xehetasuna:

Bereziki diseinatutako HTTP/2-ren eskaeren sekuentzia batek CPUaren erabilpen altu bat eragin lezake hainbat segundoz. Horrelako eskaeren kopuru aski bat egingo balitz HTTP/2 konexio konkurrenteetan, gerta liteke zerbitzariak erantzuteari uztea. Ahultasun horretarako CVE-2020-11996 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Apache, Ahultasuna

Egiaztatze okerra Palo Alto Networks enpresako PAN-OS sistemaren sinadura kriptografikoan

Argitalpen data: 2020/06/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

PAN-OS, bertsioak::

- 9.1.3 aurrekoak;
- 9.0.9 aurrekoak;
- 8.1.15 aurrekoak;
- 8.0.*.

Azalpena:

Cyber Risk and Resilience Team taldeko Salman Khan, eta Identity Services Team taldeko Cameron Duck ikertzaileek (Monash University) larritasun kritikoko ahultasun bat atzeman dute, sinadura kriptografikoaren egiaztatze okerraren arlokoa.

Konponbidea:

Ahultasuna honako bertsioen eta ostekoen bidez konpontzen da: PAN-OS 8.1.15, PAN-OS 9.0.9, PAN-OS 9.1.3.

Xehetasuna:

SAML (Security Assertion Markup Language) egiaztatzea aktibatuta dagoenean eta *Validate Identity Provider Certificate* aukera

desgaituta, PAN-OS sistemako SAML baimentzean sinadura egiaztatze okerra gertatzearen ondorioz, baimendu gabeko erasotzaile batek sareko baliabide babestuetara sartzeko izango luke. Erasotzaileak zerbitzarirako sare-sarbidea eduki beharko luke, ahultasun hori baliatzeko. Arazo hori ezin izango da baliatu SAML sistema ez bada egiaztapenerako erabiltzen. Ahultasun horretarako, CVE-2020-2021 identifikatzailea esleitu da.

Etiketak: Eguneraketa, Ahultasuna