2020ko martxoaren Bulletina

Ohartarazpenak - Teknikoak

Fidagarriak ez diren datuen deserializazioa Dell produktuetan

Argitalpen data: 2020/03/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Dell EMC Avamar Server, 7.4.1, 7.5.0, 7.5.1, 18.2, 19.1 eta 19.2 bertsioak;
- Dell EMC Integrated Data Protection Appliance (IDPA), 2.0, 2.1, 2.2, 2.3, 2.4 eta 2.4.1 bertsioak.

Azalpena:

Dell EMC Avamar Server-ek eta Dell EMC Integrated Data Protection Appliance-k duten ahultasun baten berri argitaratu da. Hori baliatuz erasotzaile batek arriskuan jar lezake kaltetutako sistema.

Konponbidea:

Ondoko hotfix-ak aplikatzea, kaltetutako bertsioaren arabera:

- Dell EMC Avamar Server 7.4.1 - HOTFIX 316625,
- Dell EMC Avamar Server 7.5.0 - HOTFIX 316626,
- Dell EMC Avamar Server 7.5.1 - HOTFIX 316627,
- Dell EMC Avamar Server 18.2 - HOTFIX 316484,
- Dell EMC Avamar Server 19.1 - HOTFIX 316485,
- Dell EMC Avamar Server 19.2 - HOTFIX 316691,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.0 - HOTFIX 316625,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.1 - HOTFIX 316626,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.2 -HOTFIX 316627,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.3 - HOTFIX 316484,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.4 - HOTFIX 316484,
- Dell EMC Integrated Data Protection Appliance (IDPA) 2.4.1 - HOTFIX 316484.

Xehetasuna:

Fidagarriak ez diren datuen deserializazio erako ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek sisteman kodea exekutatuko lukeen *payload* serializatu bat bidal lezake. Ahultasun horretarako CVE-2020-5341 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Informazioaren zabalkundea HPEren OneView Global Dashboard-en

Argitalpen data: 2020/03/04

Garrantzia: Altua

Kaltetutako baliabideak:

HPE OneView Global Dashboard, 1.9 bertsioa.

Azalpena:

HPEk kritikotasun altuko ahultasun bat aurkitu du. Urruneko erasotzaile batek sistemaren informazioa ezagutzera eman lezake.

Konponbidea:

HPE OneView Global Dashboard 1.91 bertsiora eguneratzea.

Xehetasuna:

OneView Global Dashboard-en 1.9 bertsioa instalatu ondoren, gailuak firewall atakak irekita utz litzake. Urruneko erasotzaile batek sistemaren informazioa ezagutzera eman lezake. Ahultasun horretarako CVE-2020-7130 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, HP, Ahultasuna

Hainbat ahultasun Netgear-en produktuetan

Argitalpen data: 2020/03/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- R7800, *firmwarearen* 1.0.2.68 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6400v2, *firmwarearen* 1.0.4.84 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6700, *firmwarearen* 1.0.2.8 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6700v3, *firmwarearen* 1.0.4.84 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6900, *firmwarearen* 1.0.2.8 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7900, *firmwarearen* 1.0.3.10 bertsioa baino lehenagokoak exekutatzen dituenean;
- D6220, *firmwarearen* 1.0.0.52 bertsioa baino lehenagokoak exekutatzen dituenean;
- D6400, *firmwarearen* 1.0.0.86 bertsioa baino lehenagokoak exekutatzen dituenean;
- D7000v2, *firmwarearen* 1.0.0.53 bertsioa baino lehenagokoak exekutatzen dituenean;
- D8500, *firmwarearen* 1.0.3.44 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6220, *firmwarearen* 1.1.0.80 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6250, *firmwarearen* 1.0.4.34 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6260, *firmwarearen* 1.1.0.64 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6400, *firmwarearen* 1.0.1.46 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6700v2, *firmwarearen* 1.2.0.36 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6800, *firmwarearen* 1.2.0.36 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6900P, *firmwarearen* 1.3.1.64 bertsioa baino lehenagokoak exekutatzen dituenean;
- R6900v2, *firmwarearen* 1.2.0.36 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7000, *firmwarearen* 1.0.9.42 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7000P, *firmwarearen* 1.3.1.64 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7100LG, *firmwarearen* 1.0.0.50 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7300DST, *firmwarearen* 1.0.0.70 bertsioa baino lehenagokoak exekutatzen dituenean;
- R7900P, *firmwarearen* 1.4.1.30 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8000, *firmwarearen* 1.0.4.28 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8000P, *firmwarearen* 1.4.1.30 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8300, *firmwarearen* 1.0.2.128 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8500, *firmwarearen* 1.0.2.128 bertsioa baino lehenagokoak exekutatzen dituenean;
- R8900, *firmwarearen* 1.0.4.12 bertsioa baino lehenagokoak exekutatzen dituenean;
- R9000, *firmwarearen* 1.0.4.12 bertsioa baino lehenagokoak exekutatzen dituenean;
- XR500, *firmwarearen* 2.3.2.32 bertsioa baino lehenagokoak exekutatzen dituenean.

Azalpena:

Netgear-ek bere produktuei eragiten dieten 3 ahultasunen berri eman du, bat larritasun kritikokoa eta 2 larritasun altukoak.

Konponbidea:

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

Xehetasuna:

- Larritasun kritikoko ahultasuna baliatuz, urruneko erasotzaile batek kodearen exekuzioa egin lezake autentifikatu behar izan gabe.
- Larritasun altuko ahultasun bat aurkitu da, komandoen injekzio erakoa autentifikazioaren aurretik.
- Larritasun altuko beste ahultasun bat aurkitu da, komandoen injekzio erakoa autentifikazioaren ondoren.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun Cisco-ren produktuetan

Argitalpen data: 2020/03/05

Garrantzia: Altua

Kaltetutako baliabideak:

- Cisco Prime Network Registrar, 10.1 baino lehenagoko bertsio guztiak;
- Cisco Webex Meetings, WBS 39.5.17 edo WBS 39.11.0 bertsioak baino lehenagoko Webex Network Recording Player eta Webex Player-en bertsio guztiak;
- Cisco Webex Meetings Online, 1.3.49 bertsioa baino lehenagoko Webex Network Recording Player eta Webex Player-en bertsio guztiak;
- Cisco Webex Meetings Server, 3.0MR3SecurityPatch1 eta 4.0MR2SecurityPatch2 bertsioak baino lehenagoko Webex Network Recording Player-en bertsio guztiak;
- Cisco Intelligent Proximity aplikazioa;
- Cisco Jabber;
- Cisco Webex Meetings;
- Cisco Webex Teams;
- Cisco Meeting App.

Azalpena:

Ciscok, beste ikertzaile batzuekin lankidetzan, hainbat produkturi eragiten dioten kritikotasun altuko lau ahultasun aurkitu ditu. Autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake, trafikoa atzeman edo gailuaren konfigurazioak aldatu.

Konponbidea:

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

Xehetasuna:

- Microsoft Windows-erako Cisco Webex Network Recording Player eta Cisco Webex Player-ek bi ahultasun dituzte. Horien jatorria Webex-en grabazioen barnean elementu jakin batzuk modu nahikoan ez baliozkotzea da. Urruneko erasotzaile batek kode arbitrarioa exekuta lezake sisteman. Ahultasun horietarako CVE-2020-3127 eta CVE-2020-3128 identifikatzaileak erabili dira.
- Cisco Prime Network Registrar ahula da Coss-site Request Forgery erako eraso baten aurrean. Urruneko erasotzaile batek aldaketak egin litzake gailuaren konfigurazioan. Ahultasun horretarako CVE-2020-3148 identifikatzailea erabili da.
- Cisco Webex-en Cisco Intelligent Proximity-ren SSLren inplementazioan dagoen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek Man in the middle erako eraso bat egin lezake eta trafikoa atzeman. Ahultasun horretarako CVE-2020-3155 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Bufferraren gainezkatzea Point-to-Point Protocol Daemon-en

Argitalpen data: 2020/03/06

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Daemon pppd *(Point to Point Protocol Daemon)*, 2.4.2 bertsiotik 2.4.8ra bitartean.

Azalpena:

IOActive-ko Ilja Van Sprundel ikertzaileak larritasun kritikoko ahultasun bat aurkitu du pppd deabruari eragiten diona. Autentifikatu gabeko urruneko erasotzaile batek bufferraren gainezkatzea eragin lezake eta horrela kode arbitrarioa eragin sisteman.

Konponbidea:

Eskuragarri dagoen pppd-ren azken partxea aplikatu, bere konfigurazioen arabera. Informazio gehiago eskuratzeko *Erreferentziak* atala irakurri.

Xehetasuna:

pppd deabruan *Extensible Authentication Protocol*-en (EAP) paketeen prozesatzeak duen akats baten ondorioz, autentifikatu gabeko urruneko erasotzaile batek bufferraren gainezkatzea eragin lezake, eta horrela sisteman kode arbitrarioa exekuta lezake. Ahultasun horretarako CVE-2020-8597 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Zerbitzuaren ukapena IBMren Spectrum Scale-n

Argitalpen data: 2020/03/09

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Spectrum Scale, bertsio guztiak.

Azalpena:

Fortinet-eko Honggang Ren ikertzaileak kritikotasun altuko ahultasun baten berri eman dio IBMri, IBM Spectrum Scale-ren bertsio guztiei eragiten diena. Urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake.

Konponbidea:

IBM-k ahultasuna arintzen duten hainbat eguneraketa argitaratu ditu, kaltetutako produktuaren eta bertsioaren arabera.

- IBM Spectrum Scale, V5.0.0.0 bertsiotik 5.0.4.2 bertsiora bitartean, V5.0.4.3 bertsiora eguneratzea,
- IBM Spectrum Scale, V4.2.0.0 bertsiotik 4.2.3.19 bertsiora bitartean, V4.2.2.20 bertsiora eguneratzea.

Segurtasun eguneraketak ezin aplikatuz gero, harremanetan jarri IBMren arreta zerbitzuarekin.

Xehetasuna:

Ahultasuna Spectrum Scale-ren fitxategien sisteman dago. Urruneko erasotzaile batek zerbitzuaren ukapen egoera eragin lezake Spectrum Scale-k kudeatutako sistemetan. Ahultasun horretarako CVE-2020-4217 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Kodearen urruneko exekuzioa ManageEngine-ren

Desktop Central-en

Argitalpen data: 2020/03/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

ManageEngine Desktop Central, 10.0.473 eta lehenagoko bertsioak.

Azalpena:

Source Incite-ko Steven Seeley-k larritasun kritikoko ahultasun bat aurkitu du. Hori baliatuz urruneko erasotzaile batek kaltetutako sistemaren kontrola har lezake.

Konponbidea:

Kaltetutako produktua 10.0.479 bertsiora eguneratzea.

Xehetasuna:

Ahultasun hau baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake ManageEngine Desktop Central-en kaltetutako instalazioetan. Ahultasun hau baliatzeko ez dago autentifikazioaren beharrik. Arazoaren arrazoia da erabiltzaileak emandako datuak ondo ez baliozkotzea, eta horrek datu ez-fidagarrien deserializazioa eragin dezake. Ahultasun horretarako CVE-2020-10189 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Microsoften 2020ko martxoko segurtasun buletina

Argitalpen data: 2020/03/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows;
- Microsoft Edge (EdgeHTMLn oinarritua);
- Microsoft Edge (Chromium-en oinarritua);
- ChakraCore;
- Internet Explorer;
- Microsoft Exchange Server;
- Microsoft Office, Microsoft Office Services eta Web Apps;
- Azure DevOps;
- Windows Defender;
- Visual Studio;
- Open Source Software;
- Azure;
- Microsoft Dynamics;
- Microsoft Server Message Block 3.1.1 (SMBv3), Windows 10 eta Windows Server-en; 1909 eta 1903 bertsioak.

Azalpena:

Segurtasun eguneraketei buruzko Microsoften martxoko argitalpenean 114 ahultasun jaso dira, 26 kritiko gisa sailkatu dira eta 88 garrantzitsu gisa.

GARRANTZITSUA: aipu berezia behar du SMBv3ri eragiten dion larritasun kritikoko ahultasun batek.

Konponbidea:

Dagozkien segurtasun eguneraketak instalatzea. Microsoft-en orrialdean eguneraketa horiek egiteko metodo ezberdinei buruzko argibideak daude.

GARRANTZITSUA: CVE-2020-0796 identifikatzailea duen SMBv3ren ahultasunak ez dauka eguneraketarik aurkitutako akatsa arintzeko, baina Microsoftek gomendio batzuk argitaratu ditu partxea argitaratu bitartean:

- SMBv3ren konpresioa desgaitzea zerbitzarietan:
  - SMBv3 Server, PowerShell-en ondoko lerroa exekutatzea, honek ez du prebenitzen ahultasuna baliatzea SMB bezeroetan:
    - *Set-ItemProperty -Path "HKLM:SYSTEMCurrentControlSetServicesLanmanServerParameters" DisableCompression -Type DWORD -Value 1 -Force*
  - Gainera TCP 445 ataka blokeatzea gomendatzen da.

Xehetasuna:

Argitaratutako ahultasun motak honako hauek dira:

- kodearen urruneko exekuzioa,
- pribilegioen eskalatzea,
- zerbitzuaren ukapena,
- informazioaren zabalkundea,
- identitatea ordeztea (spoofing),
- informazioa manipulatzea (tampering).

GARRANTZITSUA: Microsoft SMBv3-k CVE-2020-0796 kodeaz identifikatutako ahultasun bat dauka protokoloaren eskaera jakin batzuk kudeatzeko orduan. Autentifikatu gabeko erasotzaile batek asmo gaiztoko kodea exekuta lezake kaltetutako ekipoan. Ahultasun hau modu masiboan balia liteke.

Etiketak: Eguneraketa, Microsoft, Nabigatzailea, Ahultasuna, Windows

---

SAPen 2020ko martxoko segurtasun eguneraketa

Argitalpen data: 2020/03/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Solution Manager (User Experience Monitoring eta Diagnostics Agent), 7.2 bertsioa;
- SAP Business Client, 6.5 bertsioa;
- SAP NetWeaver:
  - UDDI Server (Services Registry), 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
  - AS ABAP Business Server Pages (Smart Forms) SAP_BASIS, 7.00, 7.01, 7.02, 7.10, 7.11, 7.30, 7.31, 7.40, 7.50, 7.51, 7.52, 7.53 eta 7.54 bertsioak;
  - Application Server Java (User Management Engine), 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50 bertsioak.
- SAP Business Objects Business Intelligence Platform(Crystal Reports), 4.1 eta 4.2 bertsioak;
- SAP Disclosure Management, 10.1 bertsioa;
- SAP BusinessObjects Mobile (MobileBIService), 4.2 bertsioa;
- SAP MaxDB (liveCache), 7.8 eta 7.9 bertsioak;
- SAP Commerce Cloud:.
  - Testweb Extension, 6.6, 6.7, 1808, 1811 eta 1905 bertsioak;
  - SmartEdit Extension, 6.6, 6.7, 1808 eta 1811 bertsioak.
- SAP ERP (EAPPGLO), 607 bertsioa;
- SAP Enable Now, 1911 baino lehenagoko bertsioak;
- SAP Fiori Launchpad, 753 eta 754 bertsioak;
- SAP Cloud Platform Integration for Data Services, 1.0 bertsioa;
- SAP Treasury eta Risk Management (Transaction Management), EA-FINSERV 600, 603, 604, 605, 606, 616, 617, 618, 800, S4CORE 101, 102, 103 eta 104 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 16 segurtasun ohar eman ditu ezagutzera. Horietatik 2 ohar lehenagotik argitaratutako segurtasun oharrei dagozkien eguneraketak dira, beste 3 larritasun kritikokoak dira, beste 3 larritasun altukoak, eta beste 10 larritasun ertainekoak.

Argitaratutako ahultasun motak honako hauek dira:

- XSS (*Cross-Site Scripting*) erako 4 ahultasun,
- autentifikazioaren egiaztapen gabeziako 3 ahultasun,
- egiaztapen gabeziako 2 ahultasun,
- SQL injekzioko ahultasun bat,
- kodearen urruneko exekuzioaren (RCE) erako ahultasun bat,
- bideetara kontrolatu gabeko sarbide erako ahultasun bat,
- zerbitzuaren ukapen erako (DoS) ahultasun bat,
- beste era batzuetako 5 ahultasun.

Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2020-6207, CVE-2020-6198, CVE-2020-6203, CVE-2020-6208, CVE-2020-6209, CVE-2020-6196, CVE-2018-2450, CVE-2020-6201, CVE-2020-6205, CVE-2020-6202, CVE-2020-6199, CVE-2020-6178, CVE-2020-6210, CVE-2020-6206, CVE-2020-6204 eta CVE-2020-6197.

Etiketak: Eguneraketa, SAP, Ahultasuna

Joomla! 3.9.16ren segurtasun eguneraketa

Argitalpen data: 2020/03/11

Garrantzia: Txikia

Kaltetutako baliabideak:

- Joomla! CMS, honako bertsioak:
  - 1.7.0 bertsiotik 3.9.15 bertsiora bitartekoak;
  - 3.2.0 bertsiotik 3.9.15 bertsiora bitartekoak;
  - 3.0.0 bertsiotik 3.9.15 bertsiora bitartekoak;
  - 2.5.0 bertsiotik 3.9.15 bertsiora bitartekoak;
  - 3.7.0 bertsiotik 3.9.15 bertsiora bitartekoak.

Azalpena:

Joomla!-k bertsio berri bat argitaratu du, bere nukleoak dituen kritikotasun txikiko 6 ahultasun konpontzen dituena, era ezberdinekoak: SQL injekzioa, CSRF, XSS, sarbidearen kontrol okerra eta identifikatzaileen talka.

Konponbidea:

- 3.9.16 bertsiora eguneratzea.

Xehetasuna:

- SQL agindu baten aldagai batean tipoen casting faltak SQL injekzio erako ahultasun bat eragiten du "Artikulu nabarmenduak" menu frontalean. Ahultasun horretarako CVE-2020-10243 identifikatzailea erreserbatu da.
- com_templates-en irudi eragiketen egiaztapen faltak CSRF erako ahultasunak eragiten ditu. Ahultasun horretarako CVE-2020-10241 identifikatzailea erreserbatu da.

- Protostar eta Beez3-ren JavaScript-ean CSS hautatzaileen erabilpen desegokiak XSS bidezko erasoak ahalbidetzen ditu. Ahultasun horretarako CVE-2020-10242 identifikatzailea erreserbatu da.
- Komunikazio txantiloietako hainbat ekintzek ez dituzte beharrezkoak diren egiaztapenak, eta horrek hainbat eraso bektore ahalbidetzen ditu. Ahultasun horretarako CVE-2020-10238 identifikatzailea erreserbatu da.
- Erabiltzaileen taulan luzera kontrolik ez egoteak eragin dezake erabiltzaile izena edota helbide elektronikoa bikoiztuta duten erabiltzaileak sortzea. Ahultasun horretarako CVE-2020-10240 identifikatzailea erreserbatu da.
- com_fields-en SQL eremu motan sarbidearen kontrol okerrak ahalbidetzen du superadmin ez diren erabiltzeen sarbidea. Ahultasun horretarako CVE-2020-10239 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Ahultasunak Intel-en hainbat produktutan

Argitalpen data: 2020/03/11

Garrantzia: Altua

Kaltetutako baliabideak:

- Intel® Graphics Drivers, Intel® prozesagailuen hirugarren belaunaldi tik hamargarrenera bitartekoak, Windows 7, 8.1 eta 10erako, 15.40.44.5107, 15.45.29.5103, 26.20.100.7584, 15.33.49.5100 eta 15.36.38.5117 baino lehenagoko bertsioak;
- Intel® NUC eta Intel® Compute Stick (ikusi ohartarazpenean bertsio zehatza);
- BlueZ, 5.53 baino lehenagoko bertsioak;
- Intel® Smart Sound Technology, ondoko bertsioak baino lehenagokoak dituzten produktuetan:.
  - 10th Generation Intel® CoreTM i7 Processors, 3431 bertsioa;
  - 8th Generation Intel® CoreTM Processors, 3349 bertsioa.

Azalpena:

Intel-ek kritikotasun altuko 10 ahultasun, ertaineko 10 ahultasun eta baxuko ahultasun bat aurkitu ditu hainbat produktutan.

Konponbidea:

Intel-ek gomendatzen du ondoko ekintzak exekutatzea:

- Windowserako Intel® Graphics Drivers azken bertsiora eguneratzea;
- Intel® NUC eta Compute Stick eguneratzea eskuragarri dagoen azken bertsiora, ohartarazpenaren taulan azalduta dagoen moduan;
- BlueZ 5.53 edo geroagoko bertsiora eguneratzea;
- Intel Smart Sound Technology eskuragarri dagoen azken bertsiora eguneratzea.

Xehetasuna:

- Larritasun altuko ahultasunak baliatuz erasotzaile lokal batek ondoko ekintzak egin litzake (salbu eta CVE-2020-0556 ahultasunean, sarbidea albokoa baita):
  - bufferraren gainezkatzea(CVE-2020-0504 eta CVE-2020-0501);
  - sarbidearen kontrol desegokia (CVE-2020-0516 eta CVE-2020-0519):
  - bideetara kontrolatu gabeko sarbidea (CVE-2020-0520);
  - baldintzen egiaztapen desegokia (CVE-2020-0505);
  - bufferrean murrizpen desegokiak (CVE-2020-0530);
  - sarrera datuen egiaztapen desegokia (CVE-2020-0526);
  - sarbidearen kontrol desegokia (CVE-2020-0556 eta CVE-2020-0583).

Gainerako ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2020-0565, CVE-2020-0514, CVE-2020-0515, CVE-2020-0508, CVE-2020-0511, CVE-2020-0503, CVE-2020-0567, CVE-2020-0502, CVE-2020-0507, CVE-2020-0517 eta CVE-2020-0506.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Palo Alto Networks-en PAN-OS-en

Argitalpen data: 2020/03/12

Garrantzia: Altua

Kaltetutako baliabideak:

PAN-OS, 8.1.13 baino lehenagoko bertsioak.

Azalpena:

Palo Alto Networks-ek larritasun altuko 3 ahultasun argitaratu ditu. Horiek baliatuz erasotzaile lokal batek pribilegioak eskala litzake eta *shell* komandoak exekutatu.

Konponbidea:

PAN-OS 8.1.13 edo bertsio berriagoetara eguneratzea.

Xehetasuna:

- Panorama-n PAN-OS-en erregistro deabruaren formatu kateak (logd) duen ahultasun bat baliatuz, autentifikatutako erasotzaile lokal batek kode arbitrarioa exekuta lezake, shell-erako sarbide murrizpena saihestuz eta pribilegioak igoz. Ahultasun horretarako CVE-2020-1979 identifikatzailea erabili da.
- PAN-OS CLI-ko shell-eko komandoen injekzio erako ahultasun bat baliatuz, autentifikatutako erasotzaile lokal batek shell-erako sarbide murrizpena saihets lezake eta bere pribilegioak igo. Ahultasun horretarako CVE-2020-1980 identifikatzailea erabili da.
- PAN-OS-en aurreikusgarriak diren aldi baterako fitxategien izenetan dagoen ahultasun bat baliatuz, pribilegioen eskalatze lokala

egin liteke. Ahultasun horretarako CVE-2020-1981 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna TIBCO Spotfire Server-en

Argitalpen data: 2020/03/12

Importancia: Crítica

Kaltetutako baliabideak:

- AWS Marketplace-rako TIBCO Spotfire Analytics Platform, 10.8.0 eta lehenagoko bertsioak;
- TIBCO Spotfire Server, 7.11.9 eta lehenagoko bertsioak;
- TIBCO Spotfire Server, 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.3.0, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5 eta 10.3.6 bertsioak;
- TIBCO Spotfire Server, 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0 eta 10.8.0 bertsioak;
- Spotfire library.

Azalpena:

TIBCO Spotfire Server Script-ek duen arazo baten berri argitaratu da. Hori baliatuz erasotzaile batek kodea exekuta lezake urrunetik.

Konponbidea:

- AWS Marketplace-rako TIBCO Spotfire Analytics Platform 10.8.1 edo goragokoa,
- TIBCO Spotfire Server:
  - 7.11.10 edo goragokoa,
  - 10.3.7 edo goragokoa,
  - 10.8.1 edo goragokoa.

Xehetasuna:

Ahultasuna baliatuz Spotfire liburutegian idazketa baimenak lituzkeen baina "Script Author" taldeko baimenik ez lukeen erasotzaile batek liburutegian gordetako fitxategien eta objektuen atributuak alda litzake. Horrela sistemak fidagarritzat tratatuko lituzke, eta Spotfire Web Player, Analyst clients eta TERR Service-k kode arbitrarioa exekutatu ahal izango lukete prozesu horiek hasi zituen sistemako kontuak dituen pribilegio berdinekin. Ahultasun horretarako CVE-2020-9408 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun VMware-n

Argitalpen data: 2020/03/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- VMware Workstation Pro / Player (Workstation), 15.x bertsioak;
- VMware Fusion Pro / Fusion (Fusion), 11.x bertsioak;
- Windowserako VMware Horizon Client, 5.x eta lehenagoko bertsioak;
- Windowserako VMware Remote Console (VMRC), 10.x bertsioak.

Azalpena:

VMwarek hiru ahultasun argitaratu ditu, bat larritasun kritikokoa eta bi altukoak. Horiek baliatuz erasotzaile batek kodea exekuta lezake host-ean, vmnetdhcp zerbitzuaren ukapena eragin host-ean, pribilegioen eskalatze lokala egin edo beste erabiltzaile bat balitz bezala komandoak exekutatu.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- Workstation 15.5.2,
- Fusion 11.5.2,
- Windowserako Horizon Client 5.30,
- Windowserako VMRC 11.0.0.

Xehetasuna:

- Larritasun kritikoko ahultasunaren xehetasuna honakoa da:
  - VMware Workstation eta Fusion-ek use-after erako ahultasun bat daukate vmnetdhcp-en. Hori baliatuz erasotzaile batek kodea exekuta lezake ostalariaren host-ean edo zerbitzuaren ukapen egoera eragin host-aren makinan exekutatzen den vmnetdhcp-en. Ahultasun horretarako CVE-2020-3947 identifikatzailea erabili da.
- Larritasun altuko ahultasunak honakoak dira:
  - VMware Workstation eta Fusion exekutatzen duten Linux makina birtualek pribilegioen eskalatze lokal erako ahultasun bat daukate, Cortado Thinprint-ek dituen fitxategien baimen desegokien ondorioz. Ahultasuna soilik balia daiteke VMware Tools makina birtualean instalatuta badago (Workstation eta Fusion-en lehenetsitako aukera). Administratzaile sarbiderik ez duen erasotzaile batek ahultasun hori balia lezake pribilegioak eskalatzeko makina birtualean. Ahultasun horretarako CVE-2020-3948 identifikatzailea erabili da.
  - Windowserako VMware Horizon Client, VMRC eta Workstation-en, VMware USBren arbitraje zerbitzurako konfigurazio fitxategiak dituen karpeta edozein erabiltzailek gainidatz dezake. Hori baliatuz erasotzaile batek komandoak exekuta litzake beste erabiltzaile bat balitz bezala. Ahultasun horretarako CVE-2020-5543 identifikatzailea erabili da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Hainbat ahultasun Moodle-n

Argitalpen data: 2020/03/16

Garrantzia: Altua

Kaltetutako baliabideak:

- 3.8 bertsiotik 3.8.1 bertsiora bitartekoak;
- 3.7 bertsiotik 3.7.4 bertsiora bitartekoak;
- 3.6 bertsiotik 3.6.8 bertsiora bitartekoak;
- 3.5 bertsiotik 3.5.10 bertsiora bitartekoak;
- Zerbitzurik gabeko lehenagoko bertsioak.

Azalpena:

Brendan Heywood eta Tim Hunt ikertzaileek Moodle-i eragiten dioten hiru ahultasunen berri eman dute, bat kritikotasun altukoa eta bi baxukoak. Urruneko erasotzaile batek segurtasun murrizpenak saihets

Konponbidea:

Moodle-k hainbat eguneraketa argitaratu ditu, kaltetutako bertsioaren arabera:

- 3.8.2;
- 3.7.5;
- 3.6.9;
- 3.5.11.

Xehetasuna:

Larritasun altuko ahultasuna baliatuz urruneko erasotzaile batek *X-Forwarded-For* goiburuak balia litzake erabiltzaile baten IPa ordezteko eta, era horretara, IP helbideen egiaztapenak saihesteko. Ahultasun horretarako CVE-2020-1755 identifikatzailea erreserbatu da.

Larritasun baxuko ahultasunetarako CVE-2020-1754 eta CVE-2020-1756 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun VMwareren produktuetan

Argitalpen data: 2020/03/18

Garrantzia: Altua

Kaltetutako baliabideak:

- VMware Workstation Pro / Player (Workstation);
- VMware Fusion Pro / Fusion (Fusion);
- Mac-erako VMware Remote Console (Mac-erako VMRC);
- Mac-erako VMware Horizon Client;
- Windows-erako VMware Horizon Client.

Azalpena:

GRIMM-eko Jefball, FireEye Inc.eko Dhanesh Kizhakkinan eta Rich Mirch ikertzaileek bi ahultasunen berri eman dute, bat larritasun altukoa eta bestea baxukoa. Erasotzaile batek pribilegioen eskalatzea egin lezake edo zerbitzuaren ukapen egoera eragin.

Konponbidea:

VMware-k eguneraketa multzo bat argitaratu du ahultasunak arintzeko.

- Fusion, 11.X bertsioa, 11.5.2 bertsiora eguneratzea;
- Mac-erako VMRC, 11.X eta lehenagoko bertsioak, 11.0.1 bertsiora eguneratzea;
- Mac-erako Horizon Client, 5.X eta lehenagoko bertsioak, 5.4.0 bertsiora eguneratzea;
- Windows-erako Workstation, 15.X bertsioa, 15.5.2 (pro eta player) bertsiora eguneratzea;
- Windows-erako Horizon Client, 5.X eta lehenagoko bertsioak, 5.4.0 bertsiora eguneratzea.

Xehetasuna:

- Kritikotasun altuko ahultasunaren jatorria, VMware Fusion, Mac-erako VMRC eta Mac-erako Horizon Client-i eragiten diena, *setuid* bitarren erabilpen desegokia da. Erasotzaile batek pribilegioen igotzea egin lezake eta root pribilegioak eskuratu kaltetutako sisteman. Ahultasun horretarako CVE-2020-3950 identifikatzailea erabili da.
- Kritikotasun baxuko ahultasunari CVE-2020-3951 identifikatzailea esleitu zaio.

Etiketak: Eguneraketa, VMware, Ahultasuna

Hainbat ahultasun Cisco-ren produktuetan

Argitalpen data: 2020/03/20

Garrantzia: Altua

Kaltetutako baliabideak:

Ahultasun horiek Cisco-ren ondoko produktuei eragiten diete, 19.2.2 baino lehenagoko Cisco SD-WAN-en software bertsioa baino lehenagokoa exekutatzen ari badira:

- vBond Orchestrator Software,
- vEdge 100 Series Routers,
- vEdge 1000 Series Routers,
- vEdge 2000 Series Routers,
- vEdge 5000 Series Routers,
- vEdge Cloud Router Platform,
- vManage Network Management (Software eta System),
- vSmart Controller Software.

Azalpena:

Orange Group-ek hainbat produkturi eragiten dieten kritikotasun altuko 3 ahultasun aurkitu ditu. Autentifikatu gabeko erasotzaile lokal batek bufferraren gainezkatzea eragin lezake, pribilegioak igo *root* mailan eta komando arbitrarioak exekutatu kaltetutako gailuan.

Konponbidea:

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

Xehetasuna:

- Autentifikatu gabeko erasotzaile lokal batek bufferraren gainezkatzea eragin lezake bereziki diseinatutako trafikoa bidaliz kaltetutako gailura, sarrera datuen baliozkotze ez-nahiko bat baliatuta. Ahultasun horretarako CVE-2020-3264 identifikatzailea erreserbatu da.
- Autentifikatu gabeko erasotzaile lokal batek root pribilegioak altxa litzake bereziki diseinatutako eskaera bat bidaliz kaltetutako sistema eragilera, sarrera datuen baliozkotze ez-nahiko bat baliatuta. Ahultasun horretarako CVE-2020-3265 identifikatzailea erreserbatu da.
- Autentifikatu gabeko erasotzaile lokal batek komando arbitrarioen injekzio bat egin lezake root pribilegioekin exekutatuak izango liratekeenak, bereziki diseinatutako datuak bidaliz CLI utilitatera, sarrera datuen baliozkotze ez-nahiko bat baliatuta. Ahultasun horretarako CVE-2020-3266 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun Liferay Portal-en

Argitalpen data: 2020/03/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Liferay Portal, 6.2.5 bertsioa eta lehenagokoak;
- Liferay Portal, 7.0.0 bertsioa eta lehenagokoak.

Azalpena:

Liferay-k bere produktuei eragiten dieten larritasun kritikoko bi ahultasun aurkitu ditu. Autentifikatutako urruneko erasotzaile batek kode arbitrarioa exekuta lezake edo informazioa ezagutzera eman.

Konponbidea:

- Liferay Portal 6.2.5, GitHub-en eskuragarri dagoen segurtasun partxea ezartzea.
- Liferay Portal 7.0.0ren kasuan ez dago partxerik eskuragarri. Liferay-k gomendatzen du Liferay Portal 7.0.1 edo geroagoko bertsiora eguneratzea.

Xehetasuna:

- Liferay Portal 6.2.5 eta lehenagokoetan DDM txantiloiek duten ahultasun bat baliatuz, autentifikatutako urruneko erasotzaile batek, txantiloiak sortzeko eta editatzeko baimena izanez gero, atariko JVM prozesuaren bidez irakurgarria litzatekeen edozein fitxategi ikus lezake.
- Liferay Portal 7.0.0 eta lehenagokoetan DDM txantiloiek duten ahultasun bat baliatuz, autentifikatutako urruneko erasotzaile batek, txantiloiak sortzeko eta editatzeko baimena izanez gero, kode arbitrarioa exekuta lezaketen txantiloiak sor litzake.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna Drupal-en core-an

Argitalpen data: 2020/03/20

Garrantzia: Ertaina

Kaltetutako baliabideak:

- 8.8.x;
- 8.7.x.

Azalpena:

Drupal proiektuak erabiltzen duen hirugarren batzuen liburutegi batek beharrezkoa zen segurtasun hobekuntza bat argitaratu du, bere konfigurazio batzuk babesteko.

Konponbidea:

8.8.4 edo 8.7.12 bertsioetara eguneratzea, eta bertan jasotzen da CKEditor-en 4.14 eguneraketa.

Ahultasuna arintzeko CKEditor modulua desgaitu egin daiteke gunea eguneratu arte.

Xehetasuna:

Drupal konfiguratuta badago CKEditor WYSIWYG-en erabilpena baimentzeko, erasotzaile batek XSS erako erasoak egin litzake beste erabiltzaile batzuen aurka, administratzaileak barne, hainbat pertsonek edukiak edita ditzaketenean.

Etiketak: Eguneraketa, CMS, Ahultasuna

Objektuen sorkuntza ez-seguru erako ahultasuna Ruby-n

Argitalpen data: 2020/03/20

Garrantzia: Altua

Kaltetutako baliabideak:

JSON gem, 2.2.0 edo lehenagoko bertsioak.

Azalpena:

Jeremy Evans ha descubierto una vulnerabilidad de severidad alta en la gema JSON de Ruby, que permitiría la creación de objetos arbitrarios en el sistema afectado.

Konponbidea:

JSON gema 2.3.0 edo bertsio berriagoetara eguneratzea.

Xehetasuna:

Hainbat JSON dokumentu aztertzean, JSON gema (Ruby-rekin datorrena barne) behartua izan liteke sisteman objektu arbitrarioak sortzera. Ahultasun horretarako CVE-2020-10663 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Ahultasuna PHP 7-n

Argitalpen data: 2020/03/20

Garrantzia: Altua

Kaltetutako baliabideak:

PHP 7, 7.4.4 baino lehenagoko bertsio guztiak.

Azalpena:

PHPk kritikotasun altuko ahultasun bat aurkitu du. Urruneko erasotzaile batek informazio sentikorra eskura lezake edo datuen injekzioa egin.

Konponbidea:

PHP 7 7.4.4 bertsiora edo berriagoetara eguneratzea.

Xehetasuna:

get_headers() funtzioak isilean trunkatzen du URLan byte nulu bat sartzean. Urruneko erasotzaile batek informazio sentikorra eskura lezake edo datuen injekzioa egin. Ahultasun horretarako CVE-2020-7066 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, PHP, Ahultasuna

Birbideratze irekia IBM Jazz for Service Management-en

Argitalpen data: 2020/03/23

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Jazz for Service Management (JazzSM), 1.1.3 bertsioa.

Azalpena:

IBM Jazz for Service Management-ek larritasun altuko ahultasun bat dauka, birbideratze ireki erakoa.

Konponbidea:

1.1.3-TIV-JazzSM-multi-FP006 partxea instalatzea.

Xehetasuna:

IBM Jazz for Service Management ahula da birbideratze irekiaren aurrean. Ahultasun hori sortzen da aplikazio batek barneratzen dituenean erabiltzaile batek kudeatutako datuak, asmo gaiztoko birbideratze bat eduki lezaketenak.

Etiketak: Eguneraketa, IBM, Ahultasuna

Kodearen urruneko exekuzio erako ahultasunak Microsoft Windows-en

Argitalpen data: 2020/03/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Windows 10, bertsio guztiak;
- Windows 8.1, 32 eta 64 bit-eko arkitektura;
- Windows RT 8.1;
- Windows 7 Service pack 1, 32 eta 64 bit-eko arkitektura;
- Windows Server 2008 Service pack 2 eta Server Core installation, 32 eta 64 bit-eko arkitektura;
- Windows Server 2012 eta Server Core instalation;
- Windows Server 2012 R2 eta Server Core instalation;
- Windows Server 2016 eta Server Core instalation;
- Windows Server 2019 eta Server Core installation.

Azalpena:

Microsoftek larritasun kritikoko bi ahultasun aurkitu ditu. Urruneko erasotzaile batek kodea exekuta lezake sisteman.

Konponbidea:

Oraingoz ez dago ahultasun horiek arintzeko partxerik. Microsoftek gomendio sorta bat argitaratu du:

- Windows Explorer-en aurrebista panela eta xehetasunen panela desgaitzea.
- WebClient zerbitzua desgaitzea;
- ATMFD.DLL berrizendatzea. Liburutegi hori ez dago Windows 10en instalazioetan Windows 10 1709 bertsioaz geroztik.

Gomendio horiek aurrera eramateko informazio gehiago *Erreferentziak* atalean eskura daiteke, kaltetutako produktuaren arabera.

Xehetasuna:

Bi ahultasun daude Microsoft Windows-en *Windows Adobe Type Manager Library* liburutegian, bereziki sortutako *Adobe Type 1 PostScritp format* maisu anitz erako letra tipoaren erabilpen oker baten ondorioz.

Etiketak: Microsoft, Ahultasuna, Windows

SQL injekzio erako ahultasunak phpMyAdmin-en

Argitalpen data: 2020/03/24

Garrantzia: Altua

Kaltetutako baliabideak:

phpMyAdmin, 4.9.5 baino lehenagoko 4.9.x bertsioak, eta 5.0.2 baino lehenagoko 5.0.x bertsioak.

Azalpena:

hoangn144_VCS, bluebird eta Yutaka WATANABE ikertzaileek 3 ahultasunen berri eman dute, 2 larritasun altukoak eta bat ertainekoa, guztiak SQL injekzio erakoak.

Konponbidea:

4.9.5, 5.0.2 edo geroagoko bertsioak eguneratzea. Ondoko partxeak ere aplikatu daitezke:

- CVE-2020-10804:
  - 89fbcd7c39e6b3979cdb2f64aa4cd5f4db27eaad,
  - 3258978c38bee8cb4b99f249dffac9c8aaea2d80.
- CVE-2020-10802: a8acd7a42cf743186528b0453f90aaa32bfefabe.
- CVE-2020-10803:
  - 2489837213b90664aceebe4c9ac641bf167b8a97,
  - 46a7aa7cd4ff2be0eeb23721fbf71567bebe69a5,
  - 6b9b2601d8af916659cde8aefd3a6eaadd10284a.

Xehetasuna:

- Zerbitzarira sarbidea lukeen erasotzaile batek SQL injekzio erako ahultasun bat balia lezake bereziki diseinatutako erabiltzaile izen bat sortzeko eta biktima engainatzeko, erabiltzaile kontu horrekin ekintza zehatzak egin ditzan. Gainera, zerbitzarian akatsak eragin litzake MySQL-ko pasahitzak aldatu nahi dituzten eta karaktere jakin batzuk dituzten erabiltzaileentzat. Ahultasun horretarako CVE-2020-10804 identifikatzailea erabili da.
- SQL injekzio erako ahultasun bat aurkitu da, eta horretan phpMyAdmin-en barnean bilaketa ekintzetarako kontsulta jakin batzuk sortzean parametro batzuk ez dute ondo ihes egiten. Ahultasun horretarako CVE-2020-10802 identifikatzailea erabili da.

Larritasun ertaineko ahultasunerako CVE-2020-10803 identifikatzailea erabili da.

Etiketak: Eguneraketa, PHP, Ahultasuna

Bufferraren gainezkatze erako ahultasuna Dell EMC iDRAC-en

Argitalpen data: 2020/03/25

Garrantzia: Altua

Kaltetutako baliabideak:

- Dell EMC iDRAC7, 2.65.65.65 baino lehenagoko bertsioak;
- Dell EMC iDRAC8, 2.70.70.70 baino lehenagoko bertsioak;
- Dell EMC iDRAC9, 4.00.00.00 baino lehenagoko bertsioak.

Azalpena:

Dell EMC iDRAC-en hainbat bertsiok larritasun altuko ahultasun bat daukate, bufferraren gainezkatze erakoa.

Konponbidea:

Kaltetutako produktuak ondorengo bertsioetara eguneratzea, fabrikatzailearen deskargen zentroan eskuragarri:.

- Dell EMC iDRAC7, 2.65.65.65 bertsioa;
- Dell EMC iDRAC8, 2.70.70.70 bertsioa;
- Dell EMC iDRAC9, 4.00.00.00 bertsioa.

Xehetasuna:

Pilan (*stack*) oinarritutako bufferraren gainezkatze erako ahultasun bat baliatuz, Dell EMC iDRAC-en hainbat bertsiori eragiten diena, autentifikatu gabeko urruneko erasotzaile batek kaltetutako prozesua blokea lezake edo sisteman kode arbitrarioa exekutatu, bereziki diseinatutako sarrera datuak bidaliz. Ahultasun horretarako CVE-2020-5344 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Jenkins-en

Argitalpen data: 2020/03/26

Garrantzia: Altua

Kaltetutako baliabideak:

- Jenkins LTS, 2.204.5 eta lehenagoko bertsioak;
- Jenkins weekly, 2.227 eta lehenagoko bertsioak.

Azalpena:

Jenkins-ek bere *core*-ari eragiten dioten 4 ahultasun aurkitu ditu, bat kritikotasun altukoa eta hiru ertainekoak. Horiek baliatuz CSRF (*Cross-Site Request Forgery*) eta XSS (*Cross-Site Scripting*) iraunkor erako erasoak egin litezke.

Konponbidea:

- Jenkins LTS, 2.204.6 edo 2.222.1 bertsiora eguneratzea;
- Jenkins weekly, 2.228 bertsiora eguneratzea.

Xehetasuna:

- Jenkins-eko luzapen puntu batek URL zehatzetarako CSRF erako erasoen aurkako babesa modu selektiboan desgaitzea ahalbidetzen du, izan ere, Stapler web aplikazioetarako *framework*-ak bidalketa eskaera egiteko erabiltzen duen URLaren bidearen errepresentazio ezberdina jasotzen baitu. Ahultasun horretarako CVE-2020-2160 identifikatzailea erabili da.
- Larritasun ertaineko ahultasunetarako honako identifikatzaileak erabili dira: CVE-2020-2161, CVE-2020-2162 eta CVE-2020-2163.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioen eskalatze erako ahultasuna IBMren WebSphere Application Server-en

Argitalpen data: 2020/03/26

Garrantzia: Altua

Kaltetutako baliabideak:

WebSphere Application Server, 7.0, 8.0, 8.5 eta 9.0 bertsioak.

Azalpena:

IBMk WebSphere Application Server-ek duen ahultasun baten berri eman du. Hori baliatuz erasotzaile batek pribilegioen eskalatzea egin lezake.

Konponbidea:

Ondoko eguneraketak aplikatzea, bertsioaren arabera:

- V9.0.0.0 bertsiotik 9.0.5.3 bertsiora bitartekoak:

    - Interim fix-en eskakizunen arabera eguneratzea eta ondoren Interim Fix PH21511 aplikatzea, edo Fix Pack 9.0.5.4 edo ondorengoak aplikatzea (2020ko bigarren lauhilekoan eskuragarri).
- V8.5.0.0 bertsiotik 8.5.5.17 bertsiora bitartekoak:
    - Interim fix-en eskakizunen arabera eguneratzea, eta ondoren Interim Fix PH21511 aplikatzea, edo Fix Pack 8.5.5.18 edo ondorengoak aplikatzea (2020ko hirugarren lauhilekoan eskuragarri).
- V8.0.0.0 bertsiotik 8.0.0.15 bertsiora bitartekoak:
    - 8.0.0.15 bertsiora eguneratzea, eta ondoren Interim Fix PH21511 aplikatzea
- V7.0.0.0 bertsiotik 7.0.0.45 bertsiora bitartekoak:
    - 7.0.0.45 bertsiora eguneratzea, eta ondoren Interim Fix PH21511 aplikatzea.

Xehetasuna:

IBM WebSphere Application Server-ek duen ahultasun bat baliatuz erasotzaile batek pribilegioak eskalatzea lor lezake, *token*-etan oinarritutako autentifikazioa erabiltzen denean administrazio eskaera batean SOAP konektorearen gainean. Ahultasun horretarako CVE-2020-4276 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun F5 produktuetan

Argitalpen data: 2020/03/27

Garrantzia: Altua

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), honako bertsio hauek:
    - 15.0.0 - 15.0.1 eta 15.1.0.1;
    - 14.0.0 - 14.1.2;
    - 13.1.0 - 13.1.3;
    - 12.1.0 - 12.1.5;
    - 11.5.2 - 11.6.5.
- BIG-IQ Centralized Management, honako bertsioak:
    - 7.0.0;
    - 6.0.0 - 6.1.0;
    - 5.2.0 - 5.4.0.

Azalpena:

F5 produktuek dituzten hainbat ahultasun argitaratu dira. Horiek baliatuz erasotzaile batek zerbitzuaren ukapen egoera eragin lezake, pribilegioak eskalatu edo Traffic Management Microkernel (TMM) ustekabean itxi.

Konponbidea:

Bertsio bakoitzaren arabera dagokion eguneraketa aplikatzea.

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator):
    - 15.1.0;
    - 15.1.0.2;
    - 15.0.1.1;
    - 14.1.2.3;
    - 13.1.3.2;
    - 12.1.5.1.
- BIG-IQ Centralized Management, honako bertsioak:
    - Une honetan ez du eguneraketarik

Xehetasuna:

- Ezagutarazi gabeko HTTP eskaerek zerbitzuaren ukapen egoera (DoS) eragin lezakete. HTTP profila behar da eta HTTP profila erabiltzen duen edozein BIG-IP modulu kaltetuta dago. Ahultasun horretarako CVE-2016-5857 identifikatzailea erreserbatu da.
- Rol ez administratiboak dituzten erabiltzaileek, esate baterako "Gonbidatua" edo "Baliabideen administratzailea", TMOS Shell-erako (tmsh) sarbidea badute, komando arbitrarioak exekuta litzakete pribilegio altuekin, bereziki diseinatutako tmsh komando bat erabiliz. Ahultasun horretarako CVE-2020-5858 identifikatzailea erreserbatu da.
- Erasotzaile batek, bereziki diseinatutako HTTP/3 mezuen bidez, TMM berrabiatzea eta aldi baterako akatsa ematea eragin lezake, BIG-IP host-etako trafikoa prozesatzean HTTP/3 QUIC profila konfiguratuta duenean. Eskuragarritasun altuko (HA) konfigurazioek huts egingo dute erreserbako host-aren gainean. Ahultasun horretarako CVE-2020-5859 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun IBMren Spectrum Protect Plus-en

Argitalpen data: 2020/03/31

Garrantzia: Altua

Kaltetutako baliabideak:

Apache Traffic Server (ATS), honako bertsioak:

- 6.0.0 - 6.2.3;
- 7.0.0 - 7.1.8;
- 8.0.0 - 8.0.5.

Azalpena:

ZeddYu Lu-k Apache Traffic Server-ek dituen hainbat ahultasunen berri eman du. Horiek baliatuz urruneko erasotzaile batek pribilegioak eskalatzea lor lezake.

Konponbidea:

Dagokion bertsiora eguneratzea, ATSren deskargen zentrotik:

- 6.x bertsioen kasuan:
  - 7.1.9, 8.0.6 edo ondorengoak.
- 7.x bertsioen kasuan:
  - 7.1.9 edo ondorengoak.
- 8.x bertsioen kasuan:
  - 8.0.6 edo ondorengoak.

Xehetasuna:

Argitaratutako ahultasunak baimendu gabeko trafikoaren eraso eta kodifikazio zatikatu erakoak dira, eta horiek baliatuz urruneko erasotzaile batek pribilegioak eskalatzea lor lezake, HTTP eskaeren interpretazio desegoki baten ondorioz. Ahultasun horietarako CVE-2020-1944, CVE-2019-17565 eta CVE-2019-17559 identifikatzaileak erabili dira.

Etiketak: Eguneraketa, Apache, Windows

Cross Site Scripting (XSS) akatsak Tiki-Wiki Cross softwarean

Argitalpen data: 2020/03/30

Garrantzia: Ertaina

Kaltetutako baliabideak:

Tiki Wiki CMS, 20.0 bertsioa eta lehenagokoak.

Azalpena:

INCIBEk koordinatu du Tiki Wiki edukien kudeatzaileak duen ahultasun baten argitalpena, CSIRT-CVko S2Grupo-ko Pablo Sebastián Arias Rodríguez, Rubén Barberà Pérez eta Jorge Alberto Palma Reyes-ek aurkitua. Esker on berezi bat dauka CSIRT-CVko ekipoarentzat (https://www.csirtcv.gva.es), honakoek osatua: Lourdes Herrero, Maite Moreno, José Vila, Adrián Antón, Adrián Capdevila, Aurora Villegas, Eva Lleonart, Fernando Cózar, Javier García, Manuel Rosa, Mario Ortiz, Mayte Aranda, Oscar Martínez, Sergio Hernández eta Yolanda Olmedo. Eurek aurkitu zuten XSS akatsa Tiki-Wiki CMS softwarean.

CVE-2020-8966 kodea esleitu zaio ahultasun horri. CVSS v3-ren arabera 6,5eko oinarrizko puntuazioa kalkulatu da, CVSSren kalkulua honakoa izanik:
AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:H/RL:W/RC:C/CR:H/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:R/MS:U/MC:H/MI:N/MA:N

Konponbidea:

21.0 bertsiora eguneratzea.

Xehetasuna:

Goranzko osagai baten informazioa jasotzen dute php orri batzuek, baina ez ditu neutralizatzen edo oker neutralizatzen ditu "< ", " >", eta "&" bezalako karaktere bereziak. Karaktere horiek web komandoen sekuentzien elementu modura interpreta litezke, web orrialdeak prozesatzen dituen beheranzko osagai batera bidaltzen direnean.

CWE-80: Web orrialde bateko script-ekin (XSS oinarrizkoa) erlazionatutako HTML etiketen neutralizazio okerra.

Denborazko lerroa

2019/11/27 - Ikertzaileen aurkikuntza.
2020/02/04 - Ikertzaileak harremanetan jarri ziren INCIBErekin.
2020/02/21 - Tiki-Wiki Security Team-ek ahultasuna konfirmatu zion INCIBEri.
2020/02/28 - Garatzaileak konfirmatu zuen softwarearen bertsio berri bat eta partxe zuzentzailea argitaratu zirela. INCIBEk, ikertzaileek eta garatzaileak soluzioa aztertu zuten eta ohartarazpena martxoaren 31n zabaltzea erabaki zuten.
2020/03/31 - INCIBEk ohartarazpena argitaratu zuen

INCIBEn jasotako ohartarazpen guztiak "bere horretan" eskaintzen dira, xede informatzaile hutsarekin. INCIBEk ez du inolako bermerik eskaintzen horietan jasotako informazioari dagokionez. INCIBEk ez du babesten ohartarazpen honetan jasotako inolako produktu edo zerbitzu komertzialik.

Ohartarazpen honi buruzko informaziorik baduzu, harremanetan jarri INCIBErekin ahultasunen jakinarazpenean adierazten den moduan.

Etiketak: 0day, CMS, CNA, Ahultasuna

Hainbat ahultasun Vertiv Avocent UMG-4000-n

Argitalpen data: 2020/03/31

Garrantzia: Altua

Kaltetutako baliabideak:

Vertiv Avocent UMG-4000, 4.2.1.19 bertsioa.

Azalpena:

Vertiv-en Avocent UMG-4000 produktuak 3 ahultasun ditu, bat larritasun altukoa eta bi larritasun ertainekoak, komandoen injekzio eta

XSS iraunkor erakoak.

Konponbidea:

- *Trellis* plataforma erabiltzen ez duten erabiltzaileek *firmware*-aren 4.2.2.21 edo goragoko bertsioa instalatu behar dute.
- *Trellis* erabiltzen duten erabiltzaileek, 5.0.2tik 5.0.6ra bitarteko bertsioak, *firmware*-aren 4.2.0.23 bertsioa exekutatzen, dagokien partxea ezarri behar dute.
- *Trellis* 5.0.6 edo goragoko bertsioetan erabiltzen duten erabiltzaileek *firmware*-aren 4.3.0.23 bertsioa instalatu behar dute.

Xehetasuna:

- Kaltetutako produktuaren web interfazea ahula da komandoen injekzio baten aurrean, aplikazioak modu okerrean neutralizatzen duelako kodearen sintaxia exekutatua izan aurretik. Web aplikazioaren komando guztiak root modura exekutatzen direnez, hori baliatuz autentifikatutako urruneko erasotzaile batek, administratzaile kontua baldin badu, komando arbitrarioak exekuta litzake. Ahultasun horretarako CVE-2019-9507 identifikatzailea erabili da.

Larritasun ertaineko ahultasunetarako honako identifikatzaileak erabili dira: CVE-2019-9508 eta CVE-2019-9509.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun IBMren Spectrum Protect Plus-en

Argitalpen data: 2020/03/31

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Spectrum Protect Plus, 10.1.0tik 10.1.5era bitarteko bertsioak.

Azalpena:

IBM Spectrum Protect Plus-ek dituen ahultasunak argitaratu dira, autentifikazioaren saihespen, direktorioen ezabaketa arbitrario eta komandoen injekzio erakoak. Horiek baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake sisteman.

Konponbidea:

10.1.5.2199 bertsiora eguneratzea.

Xehetasuna:

- Kredentzial barneratuak egotea baliatuz, adibidez pasahitzak eta giltza kriptografikoak, erasotzaile batek kode arbitrarioa exekuta lezake sisteman. Ahultasun horretarako CVE-2020-4208 identifikatzailea erreserbatu da.
- Erabiltzaileak sartutako datuen baliozkotze desegokia baliatuz, urruneko erasotzaile batek direktorioen ezabaketa arbitrarioa egin lezake. Ahultasun horretarako CVE-2020-4214 identifikatzailea erreserbatu da.
- Erabiltzaileak sartutako datuen baliozkotze desegokia baliatuz, urruneko erasotzaile batek komando arbitrarioak exekuta litzake sisteman *root* baimenekin. Ahultasun horretarako CVE-2020-4206 identifikatzailea erreserbatu da.
- Bereziki diseinatutako eskaera bat bidaliz, autentifikatu gabeko urruneko erasotzaile batek komando arbitrarioak exekuta litzake sisteman. Ahultasun horietarako CVE-2020-4241 eta CVE-2020-4242 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, IBM, Ahultasuna