2020ko Azaroaren Bulletina

Ohartarazpenak - Teknikoak

Kodearen urrutiko exekuzioaren motako ahultasuna Oracle WebLogic Server sisteman

Argitalpen data: 2020/11/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Oracle WebLogic Server, 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 eta 14.1.1.0.0 bertsioak;

Azalpena:

Hainbat ikertzailek eta segurtasun-taldek Oracle WebLogic Server sistemari eragiten dion larritasun kritikoko ahultasun horren berri eman dute. Kodearen urrutiko exekuzioaren motakoa da.

Konponbidea:

Partxeen eskuragarritasunari buruzko Fusion Middleware (login) dokumentuan azaldutako jarraibideei kasu egitea.

Xehetasunak:

Ahultasun hori CVE-2020-14882 identifikatzailearekin erlazionatua dago, eta Oracleren eguneratze kritikoen artean (2020ko urria) jaso zen. Erraz baliatu daiteke, eta, horren bidez, baimenik gabeko erasotzaile batek, HTTPren bidez sarera sartuta, Oracle WebLogic Server sistema konprometitu dezake. Ahultasun horretarako, CVE-2020-14750 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Java, Oracle, Ahultasuna

Bufferrak gainezka egitea Windowsen kernel eremuan

Argitalpen data: 2020/11/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Windowsen bertsio guztiak, Windows 7tik aurrera, Windows 10 bertsio berrienera arte.

Azalpena:

Mateusz Jurczyk eta Sergei Glazunovlek, Google Project Zero taldekoak, 0-day ahultasun bat antzeman dute Windows sistema eragilean. Une honetan, baliteke baten bat ahultasun hori erabiltzen aritzea, pribilegioetan gora egiteko.

Konponbidea:

- Windowsen 0-day ahultasun hori zuzentzeko eguneratzea azaroaren 10ean argitaratuko da.
- Google Chromeren ahultasuna bertsio honetan partxeatu zen: 86.0.4240.111.

Xehetasunak:

Windowsen kernel kriptografiaren kontrolagailuak, Windows Kernel Cryptography Driver (cng.sys) programetarako DeviceCNG

gailu bat jarri du erakusgai erabiltzaile moduan dauden programetarako, eta IOCTL barietatea onartzen du, sarrera egitura ez tribialekin. Horren ondorioz, tokiko erasotzaile batek pribilegioetan gora egin lezake eta sandbox-etik irten. Ahultasun horretarako, CVE-2020-17087 identifikatzailea esleitu da.

Ahultasun hori baliatzeko, erasotzaileak Google Chromeko 0-day ahultasuna baliatzen ari dira aurretik. Horren identifikatzailea CVE-2020-15999 da, eta horrek Chromeren barruan kode maltzurra exekutatzeko aukera ematen die.

Etiketak: 0day, Ahultasuna, Windows.

Hainbat ahultasun SaltStack sistemaren Salt eremuan

Argitalpen data: 2020/11/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Salt, 3002 bertsioa eta aurrekoak.

Azalpena:

Trend Micro Zero Day Initiative taldeko KPC ikertzaileak antzemandako 3 ahultasunetako biren berri eman du. Ahultasun horietako bi larritasun handikoak/kritikokoak dira, eta bat baxukoa. Motak: egiaztatze omisioa eta baimen arazoak.

Konponbidea:

Honako bertsioek pakete bat izango dute eskuragarri biltegitik deskargatzeko.

- 3002.x;
- 3001.x;
- 3000.x;
- 2019.x.

Honako bertsioek partxe bat dute eskuragarri, deskargatzeko:

- 3002;
- 3001.1 eta 3001.2;
- 3000.3 eta 3000.4;
- 2019.2.5 eta 2019.2.6;
- 2018.3.5;
- 2017.7.4 eta 2017.7.8;
- 2016.11.3, 2016.11.6 eta 2016.11.10;
- 2016.3.4, 2016.3.6 eta 2016.3.8;
- 2015.8.10 eta 2015.8.13.

Xehetasunak:

- Baimendu gabeko erabiltzaile batek, Salt-en APIrako sare sarbidearekin, komandoen injekzioak egin litzake (shell injections), SSH bezeroaren bidez Salt-en APIan kodea exekutatzeko. Ahultasun horretarako, CVE-2020-16846 identifikatzailea esleitu da.
- SSH bezeroa erabiltzen denean, baimenik gabeko erabiltzaile batek sarbidea lor dezake Salt-SSH zerrenda batean ezarritako helburuen aurka komandoak exekutatzeko, eauth ez delako behar den moduan balioztatzen SSH bezeroari API bidez deitzean, beraz, eauth edo token-erako edozein balioren bidez, erabiltzaileak egiaztatzea omititu lezake. Ahultasun horretarako, CVE-2020-25592 identifikatzailea esleitu da.

Larritasun baxua duen ahultasunerako CVE-2020-17490 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Ahultasuna

Pribilegioen eskalatzea HPE OneView eta Synergy Composer sistemetan

Argitalpen data: 2020/11/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- HPE Synergy Composer, 5.0, 5.00.01, 5.00.02, 5.2, 5.20.01, 5.3, 5.4 bertsioak eta aurrekoak;
- HPE Synergy Composer2, 5.0, 5.00.01, 5.00.02, 5.2, 5.20.01, 5.3, 5.4 bertsioak;
- HP OneView, 5.0, 5.00.01, 5.00.02, 5.2, 5.20.01, 5.3, 5.4 bertsioak eta aurrekoak.

Azalpena:

Hewlett Packard Enterprise erakundeak ahultasun baten berri eman du. Horren bidez, erasotzaile batek pribilegioetan gora egin lezake, urrunetik.

Konponbidea:

OneView, Composer eta Composer2 sistemen 5.5 bertsiora eguneratzea.

Xehetasunak:

Ahultasunaren bidez, erasotzaile batek pribilegioetan gora egin lezake, urrunetik, OneView eta Synergy Composer sistemetako OneView kontu bateko erabiltzaile izanik. Ahultasun horretarako, CVE-2020-7198 identifikatzailea esleitu da.

Etiketak: Eguneratzea, HP, Ahultasuna

Sarbide baimen okerra Cisco AnyConnect Secure Mobility Client sisteman

Argitalpen data: 2020/11/05

Garrantzia: Handia

Kaltetutako baliabideak:

Ahultasun honek Cisco AnyConnect Secure Mobility Client sistemaren software bertsio guztiei eragiten die, plataforma hauetarako konfigurazio ahul bat baitauka:

- AnyConnect Secure Mobility Client Linuxerako,
- AnyConnect Secure Mobility Client MacOSerako,
- AnyConnect Secure Mobility Client Windowserako.

Konfigurazio babesgabe bat izanez gero, gaitu egin behar dira bai *Auto Update* konfigurazioa (berez gaitutakoa), baita *Enable Scripting* ere (berez desgaitutakoa).

Azalpena:

Gerbert Roitburd, Secure Mobile Networking Lab (TU Darmstadt) erakundeko ikertzaileak, ahultasun baten berri eman du. Larritasun handikoa da, sarbide okerraren balioztatze motakoa.

Konponbidea:

Ciscok ez du ahultasun horren inguruko software eguneratzerik argitaratu. Fabrikatzailearen PSIRT (Product Security Incident Response Team) taldeak badaki PoC ustiapen kodea erabilgarri dagoela ohar honetan azaldutako ahultasunerako, baina ez du azaldutako ahultasunaren asmo txarreko erabilera baten berri izan.

Ahultasun horren arintze bat Auto Update funtzionaltasuna desgaitzea da.

Xehetasunak:

Cisco AnyConnect Secure Mobility softwarearen IPC (Interprocess Communication Channel) ahultasun baten ondorioz, tokiko erasotzaile batek, baimenduta, eragin dezake erabiltzaile batek script maltzur bat exekutatzea, bereziki diseinatutako IPC mezuak bidaliz, AnyConnect bezeroaren IPC entzuleari. Ahultasun horretarako, CVE-2020-3556 identifikatzailea esleitu da.

Etiketak: Cisco, Komunikazioak, Ahultasuna

Microsoften segurtasun-eguneratzeak. 2020ko azaroa

Argitalpen data: 2020/11/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows;
- Microsoft Office, Microsoft Office Services eta Web Apps;
- Internet Explorer;
- Microsoft Edge (EdgeHTML sisteman oinarritua),,
- Microsoft Edge (Chromium sisteman oinarritua);
- ChakraCore;
- Microsoft Exchange Server;
- Microsoft Dynamics;
- Microsoft Windows Codecs Library;
- Azure Sphere;
- Windows Defender;
- Microsoft Teams;
- Azure SDK;
- Azure DevOps;
- Visual Studio.

Azalpena:

Segurtasun eguneratzeen inguruko azaroko Microsoft argitalpenean 104 ahultasun jaso dira; 16 kritiko gisa sailkatu dira, 86 garrantzitsu gisa eta 2 baxu gisa.

Konponbidea:

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

Xehetasuna:

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Zerbitzua ukatzea.
- Pribilegioak handitzea,
- Informazioa zabaltzea.
- Kodearen urrutiko exekuzioa.
- Segurtasun-neurriak saihestea,
- Nortasuna ordeztea (spoofing).
- Manipulazioa (tampering).

Etiketak: Eguneratzea, Komunikazioak, Microsoft, Nabigatzailea, Ahultasuna.

Pribilegioen eskalatzearen motako ahultasuna LogicalDoc sistemaren instalazioan

Argitalpen data: 2020/11/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

LogicalDoc 8.5.1

Azalpena:

Cisco Talos erakundeko Yuri Kramarz ikertzaileak pribilegioen eskalatze motako ahultasun bat identifikatu du dokumentuen kudeaketarako LogicalDoc sistemaren instalazioan. Erasotzaile batek aplikazioak kargatutako instalazio karpetako DLL artxiboetako edozein ordeztu lezake, eta SYSTEM pribilegioak lortu.

Konponbidea:

8.5.2 bertsiora eguneratzea gomendatzen da.

Xehetasuna:

Aurkitutako ahultasunak pribilegioetan gora egiteko aukera ematen du; izan ere, instalazio karpeta 'C:LogicalDOC' da berez, eta sisteman baimendutako erabiltzaileek fitxategiak alda litzakete, gero SYSTEM authority pribilegioekin exekutatuko direnak, eta sisteman pribilegioetan gora egin. Ahultasun horretarako, CVE-2020-13542 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Pribilegioen eskalatzea Intel produktuetan

Argitalpen data: 2020/11/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Intel® CSME e Intel® AMT, 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 eta 14.5.25 bertsioen aurrekoak;
- Intel® TXE, 3.1.80 eta 4.0.30 bertsioen aurrekoak;
- Intel® Server Platform Services, SPS_E5_04.01.04.400, SPS_E3_05.01.04.200, SPS_E3_04.01.04.200, SPS_SoC-X_04.00.04.200 eta SPS_SoC-A_04.00.04.300 firmware bertsioen aurrekoak.
- Honako firmware bertsioak dagoeneko ez dira bateragarriak: Intel® ME 3.x - 10.x, Intel® TXE 1.x - 2.x eta Intel® Server Platform Services 1.x - 2.X. Ez dago bertsio hauetarako eguneratzerik aurreikusita.
- Intel® Wireless Bluetooth®:
  - Intel® Wi-Fi 6 AX201,
  - Intel® Wi-Fi 6 AX200,
  - Intel® Wireless-AC 9560,
  - Intel® Wireless-AC 9462,
  - Intel® Wireless-AC 9461,
  - Intel® Wireless-AC 9260,
  - Intel® Dual Band Wireless-AC 8265,
  - Intel® Dual Band Wireless-AC 8260,
  - Intel® Dual Band Wireless-AC 3168,
  - Intel® Wireless 7265 (Rev D) Family,
  - Intel® Dual Band Wireless-AC 3165.

Azalpena:

Intelek larritasun kritikoko 2 ahultasunen berri eman du. Motak: mugetatik kanpoko irakurketa eta bufferraren mugatze desegokia.

Konponbidea:

- Intel® CSME, Intel® TXE, Intel® AMT eta Intel® SPS erabiltzaileei gomendatzen zaie azken bertsiora eguneratzea.
- Intel® AMT SDK, prest dago deskargatzeko.
- Intel® DAL SDK sistemak ez dauka laguntza-talderik, erabiltzeari uztea eta desinstalatzea gomendatzen da.
- Intel® Wireless Bluetooth® produktuak 21.110 bertsiora edo osteko batera eguneratzea.

Xehetasuna:

- IPv6 sistemako mugetatik kanpoko idazketaren bidez, baimenik gabeko erasotzaile batek pribilegioetan gora egin lezake, sarerako sarbidearen bidez. Ahultasun horretarako, CVE-2020-8752 identifikatzailea esleitu da.
- Bufferraren mugatze okerraren bidez, baimenik gabeko erasotzaile batek pribilegioetan gora egin lezake, ondoko sarbide batetik. Ahultasun horretarako, CVE-2020-12321 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

2020ko azaroko SAP segurtasun-eguneratzea

Argitalpen data: 2020/11/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Solution Manager (JAVA stack eta User Experience Monitoring), 7.2 bertsioa;
- SAP Data Services, 4.2 bertsioa;
- SAP AS ABAP(DMIS), 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752 eta 2020 bertsioak;
- SAP S4 HANA, 100, 101, 102, 103, 104 eta 105 bertsioak;
- SAP NetWeaver, 7.20, 7.30, 7.31, 7.40, 7.50, 7.51, 7.52, 7.53, 7.54, 7.55 eta 7.82 bertsioak;
- SAP Fiori Launchpad (News Tile Application), 750, 751, 752, 753, 754 eta 755 bertsioak;
- SAP Commerce Cloud, 1808, 1811, 1905 eta 2005 bertsioak;
- BANKING SERVICES FROM SAP 9.0 (Bank Analyzer), 500 bertsioa;
- S/4HANA FIN PROD SUBLDGR, 100 bertsioa;
- SAP Process Integration (PGP Module ? Business-to-Business Add On), 1.0 bertsioa;
- SAP ERP Client, E-Bilanz 1.0 sistemarako, 1.0 bertsioa;
- SAP ERP, 600, 602, 603, 604, 605, 606, 616, 617 eta 618 bertsioak;
- SAP 3D Visual Enterprise Viewer, 9. Bertsioa.

Azalpena:

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

Konponbidea:

SAP laguntza bisitatu eta eguneratze edo partxeak instalatzea, fabrikatzaileak adierazitakoaren arabera.

Xehetasuna:

SAPek, segurtasun-partxeen hileroko komunikazioan, 12 segurtasun ohar eta eguneratze 3 egin ditu. Horietako 6 larritasun kritikokoak dira, 3 handikoak eta 6 tarteko larritasunekoak.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Egiaztatzea konprobatze faltaren 5 ahultasun,
- Informazioaren dibulgazioaren arloko 4 ahultasun,
- Baimenaren konprobatze faltaren 3 ahultasun,
- Zerbitzu ukapenaren inguruko 2 ahultasun (DoS).
- Kodearen injekzioaren ahultasun bat.
- SSOO komandoetako injekzioaren motako ahultasun bat,
- Kodearen urrutiko exekuzioaren ahultasun 1 (RCE),
- Beste motaren bateko 4 ahultasun.

Segurtasun ohar nabarmenenak honakoen ingurukoak dira:

- Baimen faltaren inguruko ahultasun kritiko horiek eragin negatiboa dute LM-Service zerbitzuaren integritate eta eskuragarritasunean, baita horien mendeko lau zerbitzuetan ere. Ahultasun horietarako CVE-2020-26821, CVE-2020-26822, CVE-2020-26823 eta CVE-2020-26824 identifikatzaileak esleitu dira.
- SAP Solution Manager sistemak ez du baimenik egiaztatzen, beraz, Solution Manager sistemara konektatutako SMDA agente guztiak konprometitu daitezke. Ahultasun horretarako, CVE-2020-6207 identifikatzailea esleitu da.
- Sarbidea behar bezala egiaztatzen ez bada, baimenik gabeko erasotzaile batek eskaera maltzurrak bidal litzake, eta kodearen urrutiko exekuzioa gerta liteke. Beraz, sistemaren konfidentzialtasuna, integritatea eta eskuragarritasuna konprometitu daitezke. Ahultasun horietarako CVE-2019-0230 eta CVE-2019-0233 identifikatzaileak erreserbatu dira.
- SAP AS ABAP (DMIS) sistemaren bidez, baimendutako erasotzaile batek kode arbitrarioa injektatu lezake funtzio-moduluan. Horrela izanik, kode-injekzio bat gerta liteke, eta aplikazioan exekutatu. Ondorioz, aplikazioaren isilpekotasuna, eskuragarritasuna eta integritatea kaltetuta geratuko lirateke. Ahultasun horretarako, CVE-2020-26808 identifikatzailea esleitu da.
- Partxeak SAP NetWeaver Application Server Javako errore bat zuzentzen du. Errore hori baliatuta, SAP sisteman baimendutako erabiltzaileek sistema eragilearen komandoetan gora egin lezakete, eta, beraz, zerbitzu eta informazio pieza bakoitza guztiz konprometitu. Ahultasun horretarako, CVE-2020-26820 identifikatzailea esleitu da.
- SAP NetWeaver (Knowledge Management) sistemak scriptaren edukiaren exekuzio automatikoa artxibo batean egiteko aukera eman lezake, sartzen den erabiltzailearen pribilegioak oker filtratuz gero. Erabiltzaile horrek administrari pribilegioak baditu, scriptaren edukiaren exekuzioak sistema osoaren konfidentzialtasuna, integritatea eta eskuragarritasuna konprometitu litzake, eta horrek biltegiratutako XSS batera eramango gintuzke. Ahultasun horretarako, CVE-2020-6284 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2020-26825, CVE-2020-26809, CVE-2020-26811, CVE-2020-26819, CVE-2020-6311, CVE-2020-26814, CVE-2020-26807, CVE-2020-6316 eta CVE-2020-26817.

Etiketak: Eguneratzea, SAP, Ahultasuna

Hainbat ahultasun Citrix SD-WAN Center sisteman

Argitalpen data: 2020/11/12

arrantzia: Kritikoa

Kaltetutako baliabideak:

- Citrix SD-WAN 11.2, 11.2.2 bertsioaren aurrekoak;
- Citrix SD-WAN 11.1, 11.1.2b bertsioaren aurrekoak;
- Citrix SD-WAN 10.2, 10.2.8 bertsioaren aurrekoak;

Azalpena:

Ariel Tempelhof, Realmode Labs erakundeko ikertzaileak, larritasun kritikoko 3 ahultasunen berri eman du. Motak: direktorio mugatu baterako ibilbide sarbide desegokiaren mugatzea (*path transversal*), baimen desegokia eta sistema eragilearen komandoen injekzioa.

Konponbidea:

Ahultasunak Citrix SD-WAN Center tresnaren honako bertsioetan konpondu dira:

- Citrix SD-WAN 11.2.2 eta Citrix SD-WAN 11.2 sistemaren osteko bertsioak;
- Citrix SD-WAN 11.1.2b eta Citrix SD-WAN 11.1 sistemaren osteko bertsioak;
- Citrix SD-WAN 10.2.8 eta Citrix SD-WAN 10.2 sistemaren osteko bertsioak.

Xehetasuna:

- IP / FQDN de SD-WAN Center helbidearekin komunika daitekeen erasotzaile batek kodearen urrutiko exekuzioa egin lezake, baimenik gabe, root pribilegioekin. Ahultasun horretarako, CVE-2020-8271 identifikatzailea esleitu da.
- IP / FQDN de SD-WAN Center helbidearekin komunika daitekeen erasotzaile batek egiaztatze omisio bat egin lezake, eta emaitza gisa SD-WAN funtzionalitatea erakusgai jarri. Ahultasun horretarako, CVE-2020-8272 identifikatzailea esleitu da.
- SD-WAN Center baimena duen erasotzaile batek root erabiltzaile egiaztatu baten pribilegioak eskura litzake. Ahultasun horretarako, CVE-2020-8273 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Cisco Security Manager sistemako direktorio mugatu baterako ibilbidea oker mugatzea

Argitalpen data: 2020/11/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Cisco Security Manager, 4.21 bertsioa eta aurrekoak.

Azalpena:

Florian Hauser ikertzaileak larritasun kritikoko ahultasun horren berri eman dio fabrikatzaileari. Direktorio mugatu baterako ibilbidearen mugatze desegokiaren motakoa da (*path traversal*).

Konponbidea:

Fabrikatzaileak kaltetutako produktuaren 4.22 partxea argitaratu du ahultasun hori konpontzeko.

Xehetasuna:

Direktorioaren zeharkako karaktereen sekuentziaren balioztatze desegokiak kaltetutako gailu bati egindako eskaeren barruan eragindako ahultasunaren ondorioz, baimenik gabeko urrutiko erasotzaile batek bereziki diseinatutako pakete bat bidal lezake kaltetutako gailura, eta, horrela, informazio sentikorrerako sarbidea lortu lezake, edo artxibo arbitrarioak deskargatu. Ahultasun horretarako, CVE-2020-27130 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Cisco, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2020/11/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco IoT FND, 4.6.1 bertsioa baino lehenagokoak;
- Cisco DNA Spaces Connector, 2.2 bertsioa eta lehenagokoak;
- Cisco IMCren bertsio ahul bat exekutatzen duten Ciscoren honako produktu hauek:
  - 5000 Serieak Enterprise Network Compute System (ENCS) Platforms;
  - UCS C-Serieak Rack Servers, *standalone* moduan;
  - UCS E-Serieak Servers;
  - UCS S-Serieak Servers, *standalone moduan.*

Azalpena:

Positive Technologies-eko Nikita Abramov ikertzaileak, barne segurtasuneko beste hainbat frogarekin batera, larritasun kritikoko 3 ahultasunen berri eman du, era hauetakoak: funtzio kritikorako autentifikazio falta, sistema eragileko komandoen injekzioa, eta memoria buffer baten mugen barneko eragiketen murrizpen okerra.

Konponbidea:

Kaltetutako produktuak honako bertsioetara eguneratzea:

- Cisco IoT FND, 4.6.1 eta ondorengo bertsioak;
- Cisco DNA Spaces Connector, 2.3 bertsioa eta lehenagokoak;
- CVE-2020-3470 ahultasunerako, Fixed Releases saileko taulak kontsultatu.

Xehetasunak:

- Cisco IoT Field Network Director-en (FND) API RESTak duen ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek backend-eko datu basera sarbidea lor lezake, CSRF (Cross-Site Request Forgery) token bat eskuratzean eta API RESTaren eskaeretan erabiltzean. Horren ondorioz informazioa irakurri, aldatu edo ezabatu lezake. Ahultasun horretarako CVE-2020-3531 identifikatzailea erabili da.
- Cisco DNA Spaces Connector-en webean oinarritutako administratzaile interfazeko ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek komando arbitrarioak exekuta litzake kaltetutako gailu batean, bereziki diseinatutako HTTP eskaerak bidaliz. Ahultasun horretarako CVE-2020-3586 identifikatzailea erabili da.
- Cisco Integrated Management Controller-en (IMC) API azpisistemak dituen hainbat ahultasun baliatuz, autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake root pribilegioekin, API azpisistemara bereziki diseinatutako HTTP eskaera bat bidaliz. Ahultasun horretarako CVE-2020-3470 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Komunikazioak, IoT, Ahultasuna

Ahultasuna Drupal-en core-an

Argitalpen data: 2020/11/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Honakoak baino lehenagoko bertsioak:

- 9.0.8;
- 8.9.9;
- 8.8.11;
- 7.74.

Azalpena: Larritasun kritikoko ahultasun bat argitaratu da, kodearen urruneko exekuzio (RCE) erakoa, Drupal-en core-ari eragiten diona.

Konponbidea:

9.0.8, 8.9.9, 8.8.11 edo 7.74 bertsioetara eguneratzea.

8.8.x baino lehenagoko Drupal 8ren bertsioak bere bizitza erabilgarriaren amaieran daude, eta dagoeneko ez dute jasotzen segurtasun estaldurarik.

Gainera, gomendagarria da lehenagotik kargatutako fitxategi guztiak auditatzea, asmo gaiztoko hedapenak dauden egiaztatzeko. Zehazki, hedapen bat baino gehiago daukaten fitxategiak, esate baterako fitxategi izena .php.txt edo .html.gif dutenak, hedapenean gidoi baxurik (_) gabe. Honako fitxategi hedapenak arriskutsutzat jo behar dira, baita hedapen osagarri bat edo gehiago jarraian dauzkatenean:

- phar,
- php,
- pl,
- py,
- cgi,
- asp,
- js,
- html,
- htm,
- phtml.

Zerrenda hori ez da guztiz osoa, hortaz komeni da aipatu gabeko beste hedapen batzuen segurtasuna ebaluatzea.

Xehetasunak:

Kargatutako fitxategietako fitxategi izen batzuen saneatze desegokiak eragin lezake fitxategiak hedapen okerrekoak balira bezala interpretatzea, eta MIME mota okerra bezala balio izatea, edo PHP modura exekutatzea host konfigurazio zehatzetarako. Ahultasun horretarako CVE-2020-13671 identifikatzailea erabili da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun VMware produktuetan

Argitalpen data : 2020/11/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- VMware ESXi,
- VMware Workstation Pro / Player (Workstation),
- VMware Fusion Pro / Fusion (Fusion),
- VMware Cloud Foundation.

Azalpena:

VMwarek bi ahultasunen berri eman du, larritasun kritiko eta altukoak, aldez aurretik askatutako memoriaren erabilpen eta pribilegioen eskalatze erakoak.

Konponbidea:

Ondoko bertsio hauetako batera eguneratzea eta, arintze neurri osagarri modura, XHCI (USB 3.x) kontrolatzailea desaktibatzea.

- ESXi 7.0rako:
  - ESXi70U1b-17168206;
- ESXi 6.7rako:
  - ESXi670-202011101-SG;
- ESXi 6.5rako:
  - ESXi650-202011301-SG;
- Fusion 11.xrako:
  - 11.5.7;
- Workstation 15.xrako:
  - 15.5.7;
- VMware Cloud Foundation (ESXi) 4.xrako:
  - Eguneraketarik ez dago oraindik;
- VMware Cloud Foundation (ESXi) 3.xrako:
  - Eguneraketarik ez dago oraindik;

Xehetasunak:

- XHCI USB kontrolatzailean aldez aurretik askatutako memoriaren erabilpen erako ahultasuna baliatuz, makina birtual batean administratzailearen pribilegio lokalak lituzkeen erasotzaile batek kodea exekuta lezake host-ean exekutatzen den makina birtualaren VMX prozesua balitz bezala. Ahultasun horretarako CVE-2020-4004 identifikatzailea erabili da.
- Sistemarako deien kudeaketa desegokia baliatuz, VMX prozesuan pribilegioak lituzkeen erasotzaile batek pribilegioak eskala litzake kaltetutako sisteman. Hau soilik egin daiteke beste ahultasun batekin batera baliatuz gero, esate baterako CVE-2020-4004rekin. Ahultasun horretarako CVE-2020-4005 identifikatzailea erabili da.

Etiketak: Eguneraketa, Birtualizazioa, VMware, Ahultasuna

Komandoen injekzio erako ahultasuna VMware-ren hainbat produktutan

Argitalpen data: 2020/11/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- VMware Workspace One Access, 20.01 eta 20.10 bertsioak Linuxen;
- VMware Identity Manager, 3.3.1, 3.3.2 eta 3.3.3 bertsioak Linuxen;
- VMware Identity Manager Connector, honako bertsio hauek:
  - 3.3.2 eta 3.3.1 Linuxen;
  - 3.3.3, 3.3.2 eta 3.3.1 Windowsen.

Azalpena:

VMware-k modu pribatuan jaso du komandoen injekzio erako ahultasun kritiko bati buruzko informazioa, fabrikatzailearen hainbat produkturi eragiten diena.

Konponbidea:

VMware-k argitaratutako 81731 artikuluko Solution atalean azaldutako workaround neurriak aplikatzea.

Xehetasunak:

VMware-ren hainbat produktuk komandoen injekzio erako ahultasun bat daukate konfiguratzaile administratiboan. 8443 atakan konfigurazio panelera sareko sarbidea lukeen eta panel horretarako administratzaile konturako pasahitz baliagarria lukeen erasotzaile batek komandoak exekuta litzake murriztu gabeko pribilegioekin azpiko sistema eragilean. Ahultasun horretarako CVE-2020-4006 identifikatzailea erabili da.

Etiketak: Birtualizazioa, VMware, Ahultasuna

Segurtasun-eguneratzea: Joomla! 3.9.23

Argitalpen data: 2020/11/25

Garrantzia: Txikia

Kaltetutako baliabideak:

Joomla! CMS, bertsioak:

- 3.0.0tik 3.9.22ra;
- 2.5.0tik 3.9.22ra;
- 1.7.0tik 3.9.22ra.

Azalpena:

Joomla! Erakundeak kritikotasun txikiko 7 ahultasun konpontzeko bertsio berri bat argitaratu du. Motak: informazioa zabaltzea, direktorio mugatu baterako sarbide desegokiaren mugatzea (path traversal), SQL injekzioa, erabiltzaileen zenbaketa, Cross-site Request Forgery (CSRF) eta ACL urraketa (Access Control List).

Konponbidea:

3.9.23 bertsiora eguneratzea.

Xehetasunak:

- com_finder tresnaren autosuggestion funtzioak ez du kontuan hartzen sarbidea, beraz, informazioa zabaldu daiteke.
- Konfigurazio globalaren orriak ez du HTML irteeran informazio konfidentziala ezabatzen, egungo balioak erakutsiz.
- mod_random_image karpetako parametroak ez dauka sarrera-balioztatzerik, beraz, direktorio mugatu baterako sarbide baten mugatze desegokia egin liteke (path traversal).
- Blacklist zerrendaren konfigurazioaren filtratze desegokiaren ondorioz, erasotzaile batek SQL injekzioa burutu lezake backend erabiltzaileen zerrendan.
- Erabiltzaile-izenaren kudeaketa desegokiaren ondorioz, erasotzaile batek erabiltzaile-zenbaketa egin lezake backend delakoaren saioaren hasierako orrian.
- emailexport de com_privacy funtzioan token konprobatzea egiten ez bada, erasotzaile batek Cross-site Request Forgery motako erasoak burutu litzake (CSRF).
- ACL arauen multzoak erabili bitartean sarbide-datuak ez balioztatzearen ondorioz, erasotzaile batek ACL idazketa urratu lezake.

Etiketak: Eguneratzea, CMS, Ahultasuna

PHP kodearen exekuzio arbitrarioa Drupal core-an

Argitalpen data: 2020/11/26

Garrantzia: Altua

Kaltetutako baliabideak:

Hauen aurreko bertsioak:

- 9.0.9;
- 8.9.10;
- 8.8.12;
- 7.75.

Azalpena:

Larritasun kritikoko ahultasun bat argitaratu da, PHP kodearen exekuzio arbitrarioaren motakoa, eta Drupal-en core delakoari eragiten dio.

Konponbidea:

Bertsio hauetara eguneratzea: 9.0.9, 8.9.10, 8.8.12 edo 7.75.

Drupal 8-ren 8.8.x bertsioaren aurrekoak azkenetan daude eta ez dute segurtasun estaldurarik jasotzen.

Arazorik ez izateko, saihestu konfiantzazkoak ez diren erabiltzaileak, honako artxiboak kargatzen dituztenak: .tar; .tar.gz; .bz2 o .tlz.

Ahalik eta arinen eguneratzea gomendatzen da, izan ere, xehetasun tekniko batzuen ondorioz, ahultasun hori baliatu daiteke.

Xehetasunak:

Drupalek erabiltzen duen PEAR Archive_Tar liburutegiak segurtasun-eguneratze bat argitaratu du honako ahultasunak konpontzeko:

- *Archive_Tar* 1.4.10 bertsioaren aurrekoak. Serializazio gabeko erasotzaile bat baimentzen du, "phar:" blokeatuta dagoelako, baina "PHAR:" ez dago. Ahultasun horretarako CVE-2020-28948 identifikatzailea esleitu da.
- *rchive_Tar*, 1. 4. 10 bertsioaren aurrekoak. Artxibo izenaren desinfekzio bat aurkezten du, "://" phar erasoei heltzeko, eta, beraz, fluxuaren beste edozein paketatze-eraso ("file: //" gisa, artxiboak gainidazteko) arrakastatsua izan liteke. Ahultasun horretarako, CVE-2020-28949 identifikatzailea esleitu da.

.tar; .tar.gz; .bz2 edo .tlz, artxiboen prozesatzea eta kargari eusteko konfiguratuta dauden Drupal proiektuak mehatxupean daude, eta, gainera, ahultasun hori baliatzeko xehetasun teknikoak daude.

Etiketak: Eguneratzea, CMS, Ahultasuna