2020ko Irailaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun Liferay Portal sisteman

Argitalpen data: 2020/09/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Liferay Portal, 7.3.3 bertsioaren aurrekoak.

Azalpena:

Liferay Portal erakundeak 3 ahultasunen berri eman du, denak larritasun altu edo kritikokoak. URL konprobatze ezaren eta zerbitzu-ukapen motakoak (DoS) dira.

Konponbidea:

Honako bertsioetara eguneratzea:

- Liferay Portal 7.3 bertsiorako, Liferay Portal 7.3 CE GA4 (7.3.3) edo osteko batera eguneratzea;
- Liferay Portal 7.2 bertsiorako, konponbidea eskuragarri dago: GitHub;
- Liferay Portal 7.1 bertsiorako, konponbidea eskuragarri dago: GitHub;

Xehetasunak:

- Liferay Portal sistemak ez du URL bat deskodetzen baliabidea erabili ahal den ala ez zehaztu aurretik. Horrela izanik, urrutiko erasotzaile bat mugatutako *portlet* baliabideetara sar liteke, kodifikazio bikoitza duen URL baten bidez. Ahultasun horretarako, CVE-2020-15840 identifikatzailea erreserbatu da.
- Liferay Portal sistemak ez du *enctype* atributuaren *multipart/form*-data balioaren tamaina mugatzen POST eskaera batean. Horren ondorioz, urrutitik baimendutako erabiltzaile batek zerbitzu-ukapen motako erasoak burutu litzake, artxibo handien kargaren bidez. Ahultasun horretarako, CVE-2020-15839 identifikatzailea erreserbatu da.
- Liferay Portal sistemak birbideratzeko daukan moduluak ez du 404 akats kode bat erregistratzean sortutako URL kopurua mugatzen, beraz, urrutiko erasotzaile batek zerbitzu-ukapen motako eraso bat egin lezake, existitzen ez diren orrien eskaera errepikatuak bidaliz. Ahultasun horretarako, CVE-2020-24554 identifikatzailea erreserbatu da.

Ahultasun horiez gain, Liferay erakundeak kritikotasun txikiagoko beste batzuen berri ere eman du. Informazio gehiago nahi baduzu, kontsultatu fabrikatzailearen ahultasunen berri emateko orria.

Etiketak: Eguneratzea, CMS, Ahultasuna.

Kodearen injekzio motako ahultasuna IBM Spectrum Protect Operations Center sisteman

Argitalpen data: 2020/09/02

Garrantzia: Kritikoa

Kaltetutako baliabideak:

IBM Spectrum Protect Operations Center; bertsioak: 8.1.0.000 bertsiotik 8.1.9.xxx bertsiora, eta 7.1.0.000 bertsiotik 7.1.10.xxx bertsiora.

Azalpena:

IBM erakundeak jakinarazi du IBM Spectrum Protect Operations Center sisteman datuak esportatu aurreko balioztatze oker baten ondorioz ahultasun bat sortu dela. Horren bidez, erasotzaile batek kode arbitrarioa exekuta lezake.

Konponbidea:

Honako bertsioak instalatzea gomendatzen da: 8.1.10.000 eta 7.1.11.000.

Xehetasuna:

IBM Spectrum Protect Operations Center sisteman atzemandako ahultasunak AIX, Linux eta Windows sistemei eragiten die, eta erasotzaile batek kode arbitrarioa exekuta lezake, esportazioaren aurretik datuak oker balioztatzearen ondorioz. Ahultasun horretarako, CVE-2020-4693 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, IBM, Linux, Ahultasuna, Windows

Cisco Jabber sistemaren sarbide-balioztatze okerra Windowserako

Argitalpen data: 2020/09/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Windowserako Cisco Jabber, bertsioak:

- 12.1;
- 12.5;
- 12.6;
- 12.7;
- 12.8;
- 12.9.

Azalpena:

Watchcom erakundeko Sortland Thoresen ikertzaileak larritasun kritikoko ahultasun bat atzeman du. Sarbidearen balioztatze okerraren motakoa da, eta Windowserako Cisco Jabber sistemari eragiten dio

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneratzeak Ciscoren Software deskarga panelean deskargatu daitezke. Informazio gehiago nahi baduzu, kontsultatu Ciscoren oharreko *Fixed Releases* atala.

Xehetasunak:

Urrutiko erasotzaile batek ahultasun hori baliatu lezake kaltetutako softwarera bereziki diseinatutako XMPP mezuak bidaliz. Horrela, aplikazioak programa arbitrarioak exekutatuko lituzke Cisco Jabber bezero softwareak exekutatzen dituen erabiltzaile-kontuaren pribilegioekin, eta horrek kode arbitrarioa exekutatzea ekar lezake (RCE). Ahultasun horretarako, CVE-2020-3495 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Cisco, Jakinarazpenak, Ahultasuna, Windows.

Microsoften segurtasun buletina. 2020ko iraila

Argitalpen data: 2020/09/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows,
- Microsoft Edge (EdgeHTML-based),
- Microsoft Edge (Chromium-based),
- Microsoft ChakraCore,
- Internet Explorer,
- SQL Server,
- Microsoft JET Database Engine,
- Microsoft Office and Microsoft Office Services and Web Apps,
- Microsoft Dynamics,
- Visual Studio,
- Microsoft Exchange Server,
- SQL Server,
- ASP.NET,
- Microsoft OneDrive,
- Azure DevOps.

Azalpena:

Segurtasun eguneratzeen inguruko iraileko Microsoft argitalpenean 127 ahultasun jaso dira oraingoan; 23 kritiko gisa sailkatu dira eta 104 garrantzitsu gisa.

Konponbidea:

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

Xehetasunak:

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, Microsoft, Nabigatzailea, Ahultasuna, Windows.

Hainbat ahultasun IBMren Clous Pak System sisteman

Argitalpen data: 2020/09/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

IBM Cloud Pak System, V2.3.0.1, V2.3.1.1 bertsioak.

Azalpena:

IBM etxeak IBM Cloud Pak System sisteman atzemandako larritasun kritikoko hainbat ahultasunen berri eman du. Horien bidez, erasotzaile batek urrutiko kodea exekutatu lezake sisteman.

Solución:

IBM Cloud Pak System V2.3.2.0 bertsiora eguneratzea.

Detalle:

FasterXML jackson-databind sistemak modu desegokian erabiltzen du gadget-en serializazioaren eta tipeatzearen arteko interakzioa, br.com.anteros.dbcp.AnterosDBCPConfig sistemarekin erlazionatua (anteros-core gisa ere ezaguna). Horrela izanik, urrutiko erasotzaile batek kode arbitrarioa exekuta lezake, bereziki diseinatutako sarrerak bidaliz. Ahultasun horretarako, CVE-2020-24616 identifikatzailea esleitu da.

Etiketak: Eguneratzea, IBM, Ahultasuna

Bufferrak gainezka egitea Paloalto etxearen PAN-OS softwarean

Argitalpen data: 2020/09/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- PAN-OS 9.1, 9.1.3 bertsioaren aurrekoak;
- PAN-OS 9.0, 9.0.9 bertsioaren aurrekoak;
- PAN-OS 8.1, 8.1.15 bertsioaren aurrekoak;
- PAN-OS 8.0, bertsio guztiak.

Deskribapena:

Paloalto sistemak PAN-OS softwarearen larritasun kritikoko ahultasun bat argitaratu du. Horren ondorioz, baimenik gabeko erasotzaile batek kode arbitrarioa exekutatu lezake root baimenekin.

Konponbidea:

PAN-OS 8.1.15, PAN-OS 9.0.9, PAN-OS 9.1.3 eta osteko bertsioak eguneratzea.

PAN-OS 7.1 eta 8.0 bertsioak ez dira elkarren jarraiak, eta ez dute eguneratzerik izango.

Xehetasunak:

Bufferraren gainezkatze motako ahultasun baten bidez, baimenik gabeko erasotzaile batek kode arbitrarioa exekutatu lezake *root* baimenekin, Captive Portal atarira edo Multi-Factor Authentication interfazera eskaera maltzurrak bidaliz.

Ahultasun horretarako, CVE-2020-2040 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Pribilegioen eskalatzea Intel produktuetan

Argitalpen data: 2020/09/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Intel® AMT eta Intel® ISM, 11.8.79, 11.12.79, 11.22.79, 12.0.68 eta 14.0.39 bertsioen aurrekoak.

Azalpena:

Intelek larritasun kritikoko ahultasun baten berri eman du. Horren bidez, baimenik gabeko tokiko erasotzaile batek pribilegioetan gora egin lezake.

Konponbidea:

Eguneratu eskuragarri dagoen azken bertsiora.

Xehetasuna:

Bufferreko mugatze desegokien ondorioz, tokiko erasotzaile batek, baimenik gabe, pribilegioetan gora egin lezake, sarerako sarbidearen bidez. Ahultasun horretarako, CVE-2020-8758 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Ahultasuna

Ahultasunak Drupal etxearen core-an

Argitalpen data: 2020/09/17

Garrantzia: Altua

Kaltetutako baliabideak:

Hauen aurreko bertsioak:

- 9.0.6;
- 8.9.6;
- 8.8.10;
- 7.73.

Azalpena:

5 ahultasun atzeman dira Drupal etxearen core delakoan; bat larritasun handikoa eta besteak tarteko larritasunekoak. Motak: XSS, baimenaren omisioa eta informazioa zabaltzea.

Konponbidea:

Bertsio hauetara eguneratzea: 9.0.6, 8.9.6, 8.8.10 edo 7.73.

Drupal 8-ren 8.8.x bertsioaren aurrekoak azkenetan daude eta ez dute segurtasun estaldurarik jasotzen. 8.7.x bertsioetako atariak edo aurrekoak 8.8.10 bertsiora eguneratu beharko dira.

Xehetasunak:

Larritasun handieneko ahultasuna XSS islatuaren motakoa da. Horren bidez, urrutiko erasotzaile batek HTML adierazteko modua baliatu lezake kaltetutako formularioetarako. Ahultasun horretarako, CVE-2020-13668 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2020-13666, CVE-2020-13667, CVE-2020-13669 eta CVE-2020-13670.

Etiketak: Eguneratzea, CMS, Ahultasuna

Hainbat ahultasun Netgear produktuetan

Argitalpen data: 2020/09/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- CBR40, 2.5.0.10 bertsioaren aurreko firmwareak;

- RBK752, 3.2.15.25 bertsioaren aurreko firmwareak;
- RBR750, 3.2.15.25 bertsioaren aurreko firmwareak;
- RBS750, 3.2.15.25 bertsioaren aurreko firmwareak;
- RBK852, 3.2.16.6 bertsioaren aurreko firmwareak;
- RBR850, 3.2.16.6 bertsioaren aurreko firmwareak;
- RBS850, 3.2.16.6 bertsioaren aurreko firmwareak;
- D6200, 1.1.00.40 bertsioaren aurreko firmwareak;
- D7000, 1.0.1.78 bertsioaren aurreko firmwareak;
- R6020, 1.0.0.42 bertsioaren aurreko firmwareak;
- R6080, 1.0.0.42 bertsioaren aurreko firmwareak;
- R6050, 1.0.1.26 bertsioaren aurreko firmwareak;
- JR6150, 1.0.1.26 bertsioaren aurreko firmwareak;
- R6120, 1.0.0.66 bertsioaren aurreko firmwareak;
- R6220, 1.1.0.100 bertsioaren aurreko firmwareak;
- R6260, 1.1.0.66 bertsioaren aurreko firmwareak;
- R6700v2, 1.2.0.62 bertsioaren aurreko firmwareak;
- R6800, 1.2.0.62 bertsioaren aurreko firmwareak;
- R6900v2, 1.2.0.62 bertsioaren aurreko firmwareak;
- AC2100, 1.2.0.62 bertsioaren aurreko firmwareak;
- AC2400, 1.2.0.62 bertsioaren aurreko firmwareak;
- AC2600, 1.2.0.62 bertsioaren aurreko firmwareak;
- R7450, 1.2.0.62 bertsioaren aurreko firmwareak;
- WNR2020, 1.1.0.62 bertsioaren aurreko firmwareak;
- JGS516PE, 2.6.0.43 bertsioaren aurreko firmwareak;
- RAX40, 1.0.3.80 bertsioaren aurreko firmwareak.

Azalpena:

Netgear etxeak bere produktuei eragiten dieten larritasun kritikoko hainbat ahultasun argitaratu ditu.

Konponbidea:

Eskuragarri dagoen azken firmware bertsiora eguneratzea. Horretarako:

- Bisitatu NETGEAR laguntza orria.
- Jarri modeloaren zenbakia bilaketa-koadroan eta hautatu menu zabalgarrian.
- Produktu zehatz baten kategoria ere hauta dezakezu, eredua bilatzeko.
- Egin klik deskargatu aukeran.
- Egungo bertsioetan, hautatu firmwarearen bertsioarekin hasten den izenburua duen deskarga.
- Egin klik deskargatu aukeran.
- Egin kasu erabiltzailearen eskuliburuan, firmwarearen bertsioaren oharretan edo produktuaren laguntza teknikoko orrian jasotako jarraibideei, firmware berria instalatzeko.

Xehetasunak:

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Baimen faltaren hiru ahultasun;
- Funtzio-mailako sarbide-kontrol ezaren ahultasun bat;
- Baimenaren aurreko komando-injekzioaren 2 ahultasun;
- Administrariaren kredentzialen zabalkundearen 6 ahultasun;
- Informazio konfidentzialaren zabalkundearen arloko 2 ahultasun;
- Konfigurazio desegokiaren ahultasun bat.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Hainbat ahultasun HPE PPU UCS Meter sisteman

Argitalpen data: 2020/09/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HPE Pay Per Use (PPU) Utility Computing Service (UCS) Meter, 1.9 bertsioa.

Azalpena:

"rgod" izenez ezaguna den ikertzaileak, ZDIren Trend Micro enpresarekin elkarlanean, 3 ahultasunen berri eman du; 1 larritasun kritikokoa da, eta 2 larritasun handikoak. Motak: kodearen urrutiko exekuzioa (RCE) eta informazioa zabaltzea.

Solución:

HPEk kaltetutako produktuaren garapen-programaren jarraitutasuna eten du, eta deskarga ezabatu egin da My HPE Software Center zentrotik. Beraz, produktu hori ezabatzea gomendatzen da, zaharkituta geratu baita.

Ahultasun motei erreparatuta, arintze-estrategia bakarra aplikazioarekiko interakzioa mugatzea da.

Xehetasunak:

- Baimenik gabeko urrutiko erasotzaile batek kode arbitrarioa exekuta lezake, sistemaren testuinguruan, kaltetutako HPE PPU UCS Meter instalazioetan, ReceiverServlet motako balioztatze egokirik eza dela eta. Ahultasun horretarako, CVE-2020-24626 identifikatzailea esleitu da.
- Baimenik gabeko urrutiko erasotzaile batek informazioa zabaldu lezake, sistemaren testuinguruan, kaltetutako HPE PPU UCS Meter instalazioetan, DownloadServlet motako balioztatze egokirik eza dela eta. Ahultasun horretarako, CVE-

2020-24624 identifikatzailea esleitu da.
- Baimenik gabeko urrutiko erasotzaile batek informazioa zabaldu lezake, sistemaren testuinguruan, kaltetutako HPE PPU UCS Meter instalazioetan, ReceiverServlet motako balioztatze egokirik eza dela eta. Ahultasun horretarako, CVE-2020-24625 identifikatzailea esleitu da.

Etiketak: HP, Ahultasuna

Hainbat ahultasun Moodle sisteman

Argitalpen data: 2020/09/22

Garrantzia: Handia

Kaltetutako baliabideak:

- 3.9 bertsiotik 3.9.1 bertsiora;
- 3.8 bertsiotik 3.8.4 bertsiora;
- 3.7 bertsiotik 3.7.7 bertsiora;
- 3.5 bertsiotik 3.5.13 bertsiora;
- Bateragarriak ez diren aurreko bertsioak.

Azalpena:

Hainbat ikertzailek 5 ahultasunen berri eman dute; 3 larritasun handikoak eta 2 baxukoak. Motak: XSS biltegiratua, XSS islatua, pribilegioen eskalatzea, zerbitzu ukapena (DoS) eta JavaScript kodearen sanitizazio falta.

Konponbidea:

Moodle sistemak hainbat eguneratze argitaratu ditu, kaltetutako bertsioaren arabera:

- 3.9.2;
- 3.8.5;
- 3.7.8;
- 3.5.14.

Xehetasunak:

- moodlenetprofile erabiltzailearen profil-eremuak ez ditu sartutako datuak behar beste balioztatzen, biltegiratutako XSS eraso bat sufritzeko arriskua saihesteko. Ahultasun horretarako, CVE-2020-25627 identifikatzailea esleitu da.
- Administrazio egitekoen erregistroaren filtroak ez ditu behar beste balioztatzen sartutako datuak, XSS islatuaren motako eraso bat saihesteko. Ahultasun horretarako, CVE-2020-25628 identifikatzailea esleitu da.
- Zip artxiboen tamaina, deskonprimatuta, ez zen konprobatu deskonprimatu aurretik eskura zegoen erabiltzaile-kuotarekiko, beraz, zerbitzuaren ukapena sortu liteke (DoS). Ahultasun horretarako, CVE-2020-25630 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2020-25629 eta CVE-2020-25631.

Etiketak: Eguneratzea, CMS, Ahultasuna

Hainbat ahultasun IBM Tivoli Monitoring sisteman

Argitalpen data: 2020/09/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

IBM Tivoli Monitoring, 6.3.0 bertsioa, Fix Pack 7, Service Pack 5.

Azalpena:

IBM erakundeak 4 ahultasunen berri eman du; 3 tarteko larritasunekoak dira eta 1 larritasun kritikokoa, IHS Server eta WebSphere Application Server sistemetan. Produktu horiek, halaber, IBM Tivoli Monitoring (ITM) sisteman integratuta daude.

Konponbidea:

Partxe hau aplikatzea: 6.X.X-TIV-ITM_TEPS_EWAS-IHS_ALL_8.55.17.01 VRMF 6.3.0.x.

Xehetasunak:

- IBM WebSphere Application Server sistemaren bidez, urrutiko erasotzaile batek urrutiko kode arbitrarioa exekuta lezake sisteman, bereziki diseinatutako objektu serializatuen sekuentzia baten bidez. Larritasun handiko ahultasun horretarako CVE-2020-4450 identifikatzailea esleitu da.
- IBM WebSphere Application Server sisteman datu ordezkaritza desegokia gertatzekotan, urrutiko erasotzaile batek informazio konfidentziala lor lezake. Tarteko larritasuna duen ahultasun horretarako CVE-2019-4670 identifikatzailea esleitu da.
- Baimendutako erasotzaile batek asmo maltzurrekin diseinatutako artxibo-izen bat sortu lezake, eta hori modu desegoki batean interpretatu liteke, jsp eduki moduan, eta exekutatu. Tarteko larritasuna duen ahultasun horretarako CVE-2020-4163 identifikatzailea esleitu da.
- Apache Commons Beanutils klaseen propietateak ez badira behar den moduan ezabatzen, urrutiko erasotzaile bat sistemara sar liteke baimenik gabe. Tarteko larritasuna duen ahultasun horretarako CVE-2019-10086 identifikatzailea

esleitu da.

Etiketak: Eguneratzea, IBM, Ahultasuna