2019ko Azaroaren Bulletina

Ohartarazpenak - Teknikoak

XSS ahultasuna F5en BIG-IP TMUI-n

Argitalpen data: 2019/11/04

Garrantzia: Altua

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM eta WebAccelerator), honako bertsio hauek:
  - 13.1.0tik 13.1.3ra bitartekoak;
  - 12.1.0tik 12.1.5era bitartekoak;
  - 11.5.2tik 11.6.5era bitartekoak.

Azalpena:

The Tarantula Team-ek *cross-site scripting* (XSS) islatu erako ahultasun bat aurkitu du BIG-IP produktuaren *Traffic Management User Interface* (TMUI) osagaiaren agerrarazi gabeko orrialde batean, BIG-IPren konfigurazio utilitate modura ere ezaguna.

Konponbidea:

BIG-IP 14.0.0 bertsiora eguneratzea.

Xehetasuna:

Erasotzaile batek ahultasun hau balia lezake bereziki diseinatutako URL bat erabiliz, XSS islatu erako erasoak egiteko TMUIren segurtasun orrialdeen agerrarazi gabeko orrialde batean. Ahultasun horretarako CVE-2019-6657 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Xen-en

Argitalpen data: 2019/11/04

Garrantzia: Altua

Kaltetutako baliabideak:

- Xen, 4.6 eta ondorengo bertsioak;
- Xen, 32 bit-eko bertsioak, 3.2 bertsiotik aurrerakoak;
- Xen, x86 sistema guztiak, konfiantzarik gabeko PV gonbidatuekin;
- ostalariek gailu fisikoetara sarbide zuzena duten Xen sistema guztiak.
- Xen, ARM sistema guztiak;
- Citrix Hypervisor, 8.0 eta lehenagoko bertsioak.

Azalpena:

Xen-ek dituen hainbat ahultasun argitaratu dira. Horiek baliatuz zerbitzuaren ukapena, pribilegioen eskalatzea edo datuen hondatzea eragin litezke.

Konponbidea:

Ahultasun horiek konpontzeko argitaratutako partxeak aplikatzea gomendatzen da. Informazio gehiago eskuratzeko *Erreferentziak* atala irakurri.

Xehetasuna:

- Formatu okerra duten sarrera parametroen interpretazioak akatsa eragiten du *hypercall_create_continuation*() funtzioan, eta

ondorioz Xen ustekabean ixten da. Ahultasun horretarako CVE-2019-18420 identifikatzailea erabili da.
- 32 bit-eko erabiltzaile gonbidatuaren moduaren emulazioa baliatuz, erasotzaile batek hura instala lezake, eta ondoren berak aukeratutako deskriptoreak erabili, eta horrela pribilegioen eskalatzea egin liteke. Ahultasun horretarako CVE-2019-18425 identifikatzailea erabili da.
- Erasotzaile batek erabiltzen ari diren orrialdeko tauletan idazteko sarbide ahalmena eskura lezake pribilegioak eskalatzeko. Ahultasun horretarako CVE-2019-18421 identifikatzailea erabili da.
- Bereziki diseinatutako hiperdei batek, hiperesteka edo sarbide zuzen baten bidez kontrol egiaztapenak saihesten dituen helbide batera sarbidea lortzearekin batera, erasotzaile bati ahalbidetu liezaioke hiperbisorearen ustekabeko itxiera eragitea, eta ondorioz zerbitzuaren ukapen egoera gertatuko litzateke. Ahultasun horretarako CVE-2019-18423 identifikatzailea erabili da.
- Ostalari domeinua ixten denean edo gailua dom0 domeinuari berriro esleitzen zaionean, gailu fisiko batera sarbidea lukeen domeinu ez fidagarri batek sistemaren memoriara sartzea lor lezake irakurri edo idazteko, eta horrek pribilegioen eskalatzea eragingo luke. Ahultasun horretarako CVE-2019-18424 identifikatzailea erabili da.
- ARM sistema batean salbuespen bat gertatzen denean, etendura batzuk baldintzarik gabe gaitzen dira salbuespenak sartzen diren bitartean. Hori baliatuz erasotzaile batek datuen hondatzea, zerbitzuaren ukapena edo pribilegioak eskalatzea eragin litzake. Ahultasun horretarako CVE-2019-18422 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Joomla! 3.9.13ren segurtasun eguneraketa

Argitalpen data: 2019/11/06

Garrantzia: Txikia

Kaltetutako baliabideak:

Joomla! CMS, 3.2.0tik 3.9.12ra bitarteko bertsioak.

Azalpena:

Joomla!-k bertsio berri bat argitaratu du, bere nukleoak dituen kritikotasun txikiko bi ahultasun konpontzen dituena, *cross-site request forgery* (CSRF) eta bidearen ezagutarazte erakoak.

Konponbidea:

3.9.13 bertsiora eguneratzea.

Xehetasuna:

- *com_template*- n *token*-a ez egiaztatzeak CSRF erako ahultasun bat eragin lezake. Ahultasun horretarako CVE-2019-18650 identifikatzailea erabili da.
- *phputf8*-ren mapeatze fitxategietan sarbidearen egiaztatze falta batek bidea ezagutaraztea ahalbidetu lezake. Ahultasun horretarako CVE-2019-18674 identifikatzailea erabili da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/11/07

Garrantzia: Altua

Kaltetutako baliabideak:

- Cisco EPNM, 3.0.2 baino lehenagoko bertsioak,
- Cisco Prime Infrastructure (PI), honako bertsioak baino lehenagokoak:
  - 3.4.2,
  - 3.5.1,
  - 3.6.0 Update 02,
- Cisco RoomOS Software, RoomOS July Drop 1 2019 baino lehenagoko bertsioak,
- Cisco RoomOS Software, SSH gaituta duten RoomOS September Drop 1 2019 baino lehenagoko bertsioak,
- Routeres Cisco Small Business RV Series, firmwarearen bertsioa 4.2.3.10 baino lehenagokoa dutenak,
- Cisco TC Software, 7.3.19 baino lehenagoko bertsioak,
- Cisco TelePresence CE Software, 9.8.0 baino lehenagoko bertsioak,
- Cisco Web Security Appliance (WSA),
- Cisco Webex Meetings Online, 1.3.44 bertsioa baino lehenagoko Webex Network Recording Player eta Webex Player-en bertsio guztiak,
- Cisco Webex Meetings Server, 4.0MR2 baino lehenagoko Webex Network Recording Player-en bertsio guztiak,
- Cisco Webex Meetings sites, WBS 39.5.12 bertsioa baino lehenagoko Webex Network Recording Player eta Webex Player-en bertsio guztiak,
- Cisco Wireless LAN Controllers, 8.4tik 8.9ra bitarteko bertsioak.

Azalpena:

Ciscok bere produktuei eragiten dieten larritasun altuko 12 ahultasunen berri eman du.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Cisco Softwareren deskarga paneletik deskarga daitezke.

Xehetasuna:

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

- Komandoa exekutatzea *root* pribilegioekin,
- Zerbitzuaren ukapen egoera (DoS) eragitea,
- Administratzaile pribilegioak eskuratzea,

- Kode arbitrarioa exekutatzea,
- Pribilegioak eskalatzea.

Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2019-15283, CVE-2019-15284, CVE-2019-15285, CVE-2019-15286, CVE-2019-15287, CVE-2019-15271, CVE-2019-15956, CVE-2019-15276, CVE-2019-15288, CVE-2019-15289, CVE-2019-15957, CVE-2019-15958.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun Squid-en

Argitalpen data: 2019/11/11

Garrantzia: Altua

Kaltetutako baliabideak:

Squid-en ondoko bertsioak:

- 2.x-etik 2.7.STABLE9ra bitartekoak;
- 3.x-etik 3.5.28ra bitartekoak;
- 4.x-etik 4.8ra bitartekoak.

Azalpena:

Bost ahultasun aurkitu dira Squid proxy zerbitzariaren hainbat bertsiotan.

Konponbidea:

4.9 bertsiora eguneratzea.

Xehetasuna:

- Bufferraren kudeaketa desegokia baliatuz, erasotzaile batek pilaren gainezkatzea eragin lezake eta kodea urrunetik exekutatu URN prozesaketan. Ahultasun horretarako CVE-2019-12526 identifikatzailea erreserbatu da.
- Sarrera datuen baliozkotze desegokia baliatuz, erasotzaile batek segurtasun mekanismoak saihets litzake murriztutako HTTP zerbitzarietara sarbidea lortzeko. Ahultasun horretarako CVE-2019-12523 identifikatzailea erreserbatu da.
- Sarrera datuen baliozkotze desegokia baliatuz, erasotzaile batek bufferraren gainezkatzea eragin lezake zerbitzuaren ukapen egoera sortzeko. Ahultasun horretarako CVE-2019-12523 identifikatzailea erreserbatu da.
- *append_domain*-ekin konfiguratuta dagoenean Squid-ek mezuak modu desegokian prozesatzen dituenez, trafikoa jatorri desegokietara birbidera liteke. Ahultasun horretarako CVE-2019-18677 identifikatzailea erreserbatu da.
- Mezuen analisi okerraren ondorioz HTTP eskarien zatiketa arazo bat sor liteke. Ahultasun horretarako CVE-2019-18678 identifikatzailea erreserbatu da.
- Datuen kudeaketa okerra baliatuz, erasotzaile batek informazioa ezagutzera eman lezake HTTP Digest Authentication prozesatzean. Ahultasun horretarako CVE-2019-18679 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun VMware-ren Workstation eta Fusion-en

Argitalpen data: 2019/11/13

Garrantzia: Altua

Kaltetutako baliabideak:

- VMware Workstation Pro / Player, 15.5.1 baino lehenagoko bertsioak,
- VMware Fusion Pro / Fusion, 15.5.1 baino lehenagoko bertsioak.

Azalpena:

VMwarek hiru ahultasun aurkitu ditu, bi kritikotasun altukoak eta bestea ertainekoa. Urruneko erasotzaile batek zerbitzuaren ukapen egoera sor lezake, informazio sentikorra ezagutzera eman edo kodea exekutatu.

Konponbidea:

VMwarek ahultasunak konpontzen dituzten eguneraketak argitaratu ditu, kaltetutako produktuaren arabera.

- VMware Workstation Pro 15.5.1 bertsiora eguneratzea,
- VMware Workstation Player 15.5.1 bertsiora eguneratzea,
- VMware Fusion 15.5.1 bertsiora eguneratzea.

Xehetasuna:

Kritikotasun altuko ahultasunak honakoak dira:

- Sare birtualeko e1000e egokitzaileak duen mugaz kanpoko idazketa erako ahultasun bat baliatuz, urruneko erasotzaile batek kodea exekuta lezake *host*-ean makina birtualetik, edo zerbitzuaren ukapen egoera sor lezake makina birtualean. Ahultasun horretarako CVE-2019-5541 identifikatzailea erreserbatu da.
- *vmnetdhcp*-ek duen ahultasun baten bidez, urruneko erasotzaile batek makina birtualean *host*-aren prozesuen memoriaren informazioa eskura lezake eta *host*-aren informazio sentikorra ezagutzera emateko erabili. Ahultasun horretarako CVE-2019-5540 identifikatzailea erreserbatu da.

Kritikotasun ertaineko ahultasunerako CVE-2019-5542 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Cross-site scripting (XSS) TIBCO EBXen

Argitalpen data: 2019/11/13

Garrantzia: Altua

Kaltetutako baliabideak:

- TIBCO EBXen ondorengo bertsioetako web zerbitzaria:
  - 5.8.1.fixR eta lehenagokoak
  - 5.9.3, 5.9.4, 5.9.5 eta 5.9.6
- TIBCO EBXen osagaien (Add-ons) ondoko bertsioetako Digital Asset Manager-en web interfazean:
  - 3.20.13 eta lehenagokoak
  - 4.1.0, 4.2.0, 4.2.1 eta 4.2.2
- TIBCO EBXen osagaien (Add-ons) ondoko bertsioetako Data Exchange-ren web interfazean:
  - 3.20.13 eta lehenagokoak
  - 4.1.0

Azalpena:

TIBCOk bere hainbat produkturi eragiten dieten hiru ahultasun argitaratu ditu. Horiek baliatuz erasotzaile batek cross-site scripting (XSS) erako erasoak egin litzake.

Konponbidea:

TIBCOk arazo horiei aurre egiten dieten kaltetutako sistemen eguneraketak argitaratu ditu:

- 5.8.1.fixR eta geroagoko bertsioak 5.8.1.fixS bertsiora edo goragoko batera eguneratu behar dira.
- 5.9.3, 5.9.4, 5.9.5 eta 5.9.6 bertsioak 5.9.7 bertsiora edo goragoko batera eguneratu behar dira.
- Digital Asset Manager-en web interfazerako osagaien 3.20.13 eta geroagoko bertsioak 3.20.14 edo goragoko batera eguneratu behar dira.
- Digital Asset Manager-en web interfazerako osagaien 4.1.0, 4.2.0, 4.2.1 eta 4.2.2 bertsioak 4.3.0 edo goragoko batera eguneratu behar dira.
- Data Exchange-ren web interfazerako osagaien 3.20.13 eta geroagoko bertsioak 3.20.14 edo goragoko batera eguneratu behar dira.
- Data Exchange-ren web interfazerako osagaien 4.1.0 bertsioak 4.2.0 edo goragoko batera eguneratu behar dira.

Xehetasuna:

- Web zerbitzariak duen ahultasuna baliatuz, autentifikatutako erabiltzaileek XSS erasoak egin litzakete gordetako webguneen artean, eta autentifikatu gabeko erabiltzaileek XSS erasoak egin litzakete islatutako webguneen artean. Ahultasun horretarako CVE-2019-17330 identifikatzailea erabili da.
- Digital Asset Manager-en web interfazeko osagaiei eragiten dien ahultasuna baliatuz, autentifikatutako erabiltzaileek XSS erasoak egin litzakete gordetako webguneen artean. Ahultasun horretarako CVE-2019-17332 identifikatzailea erabili da.
- Data Exchange-ren web interfazeko osagaiei eragiten dien ahultasuna baliatuz, autentifikatutako erabiltzaileek XSS erasoak egin litzakete gordetako webguneen artean. Ahultasun horretarako CVE-2019-17331 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Intel-en produktuetan

Argitalpen data: 2019/11/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Intel Core:
  - prozesagailuen 2. belaunalditik 10.era bitartekoak;
  - m familia;
  - X-series familia.
- Intel Pentium Gold seriea;
- Intel Celeron:
  - G seriea;
  - 5000 seriea.
- Intel Xeon:
  - Scalable;
  - E familia;
  - D familia;
  - W familia;
  - legacy.
- Intel Atom C seriea;
- Intel Converged Security and Manageability Engine (CSME), Intel Active Management Technology (AMT), Intel Dynamic Application Loader (DAL) eta Intel DAL software:
  - 11.0tik 11.8.65ra bitartekoak;
  - 11.10etik 11.11.65era bitartekoak;
  - 11.20etik 11.22.65era bitartekoak;
  - 12.0tik 12.0.35era bitartekoak;
  - 13.0.0;
  - 14.0.0.
- Intel SPS:
- SPS_E5_04.00.03.199.0 bertsiotik SPS_E5_04.00.04.380.0 bertsiora bitartean;
  - SPS_SoC-X_04.00.04.051.0 bertsiotik, SPS_SoC-X_04.00.04.085.0 bertsiora bitartean;
  - SPS_SoC-A_04.00.03.065.0 bertsiotik SPS_SoC-A_04.00.04.180.0 bertsiora bitartean;
  - SPS_E3_04.01.03.021.0 bertsiotik SPS_E3_04.01.04.053.0 bertsiora bitartean.
- Intel Trusted Execution Engine (TXE):

    - 3.0 bertsiotik 3.1.65 bertsiora bitartean;
    - 4.0 bertsiotik 4.0.15 bertsiora bitartean.
- Intel Ethernet 700 Series Controller:
    - firmwarearen 7.0 bertsioa baino lehenagokoak;
    - softwarearen 24.0 bertsioa baino lehenagokoak.
- Intel WIFI Drivers eta Intel PROSet/Wireless WiFi Software, 21.40 bertsioa baino lehenagokoak ondoko produktuetan:
    - Intel Wi-Fi 6 AX201 eta AX200;
    - Intel Wireless-AC 9560, 9462, 9461 eta 9260;
    - Intel Dual Band Wireless-AC 8265, 8260 eta 3168;
    - Intel Wireless 7265 familia (Rev D);
    - Intel Dual Band Wireless-AC 3165.
- Windowserako Intel SGX SDK, honako bertsioak:
    - 2.4.100.51291 eta lehenagokoak;
    - 2.3.101.50222;
    - 2.3.100.49777.
- Linuxerako Intel SGX SDK, honako bertsioak:
    - 2.6.100.51363 eta lehenagokoak;
    - 2.5.100.49891;
    - 2.4.100.48163;
    - 2.3.100.46354;
    - 2.2.100.45311.
- Intel Server Boards, honako bertsioak: BBS2600BPB, BBS2600BPQ, BBS2600BPS, BBS2600BPBR, BBS2600BPQR, BBS2600BPSR, S2600WF0, S2600WFQ, S2600WFT, S2600WF0R, S2600WFQR, S2600WFTR, S2600STB, S2600STQ, S2600STBR, S2600STQR, BBS2600STB, BBS2600STQ, BBS2600STBR eta BBS2600STQR;
- Intel Compute Modules, honako bertsioak: HNS2600BPB, HNS2600BPQ, HNS2600BPS, HNS2600BPB24, HNS2600BPQ24, HNS2600BPS24, HNS2600BPBLC, HNS2600BPBLC24, HNS2600BPBR, HNS2600BPBRX, HPCHNS2600BPBR, HNS2600BPQR, HPCHNS2600BPQR, HNS2600BPSR, HPCHNS2600BPSR, HNS2600BPB24R, HNS2600BPB24RX, HNS2600BPQ24R, HNS2600BPS24R, HNS2600BPBLCR, HNS2600BPBLC24R, S9256WK1HLC, S9248WK1HLC, S9232WK1HLC, S9248WK2HLC, S9232WK2HLC, S9248WK2HAC eta S9232WK2HAC;
- Intel Server Systems, honako bertsioak: R1304WF0YS, R1304WFTYS, R1208WFTYS, R2308WFTZS, R2208WF0ZS, R2208WFTZS, R2208WFQZS, R2312WF0NP, R2312WFTZS, R2312WFQZS, R2224WFQZS, R2224WFTZS, R1208WFTYSR, HPCR1208WFTYSR, R1304WF0YSR, HPCR1304WF0YSR, R1304WFTYSR, HPCR1304WFTYSR, R2208WFTZSR, R2208WFTZSRX, HPCR2208WFTZSR, HPCR2208WFTZSRX, R2208WF0ZSR, HPCR2208WF0ZSR, R2224WFTZSR, HPCR2224WFTZSR, R2308WFTZSR, HPCR2308WFTZSR, R2312WFTZSR, HPCR2312WFTZSR, R2312WF0NPR, HPCR2312WF0NPR, R2208WFQZSR, HPCR2208WFQZSR, R1208WFQYSR eta HPCR1208WFQYSR.

Ahultasun horiek fabrikatzaile hauei eragiten diete, besteak beste:

- Xen: Xen-en (Intel-en oinarritutako x86 prozesagailuak) bertsio guztiak exekutatzen dituzten sistemak;
- Citrix
    - Citrix Hypervisor, 8.0 eta lehenagoko bertsioak;
    - Citrix ADC eta Citrix Gateway, ondoko MPX/SDX serieak:
        - 8900;
        - 14000-40G/14000-40S/14000-40C;
        - 15000-25G/15000-50G;
        - 25000-40G;
        - 26000/26000-50G.
- Dell: Dell EMC Servers eta Dell EMC Networking Virtual Edge Platform 4600 (VEP 4600).

Azalpena:

Intelek 12 segurtasun ohartarazpen argitaratu ditu produktuen bere segurtasun zentroan, 2 larritasun kritikokoak, 8 larritasun altukoak eta 2 larritasun ertainekoak. Ahultasun horiek Intelen osagaiak beren produktuetan erabiltzen dituzten beste fabrikatzaile batzuei ere eragiten diete.

Konponbidea:

Produktuaren azken bertsiora eguneratzea.

Xehetasuna:

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

- zerbitzuaren ukapena;
- pribilegioak eskalatzea;
- informazioa zabaltzea.

Honako identifikatzaile hauek erreserbatu dira: CVE-2018-12207, CVE-2019-0123, CVE-2019-0124, CVE-2019-0152, CVE-2019-0151, CVE-2019-0169, CVE-2019-11132, CVE-2019-11147, CVE-2019-11105, CVE-2019-11088, CVE-2019-11131, CVE-2019-11104, CVE-2019-11097, CVE-2019-11103, CVE-2019-0131, CVE-2019-11090, CVE-2019-0165, CVE-2019-0166, CVE-2019-0168, CVE-2019-11087, CVE-2019-11101, CVE-2019-11100, CVE-2019-11102, CVE-2019-11106, CVE-2019-11107, CVE-2019-11109, CVE-2019-11110, CVE-2019-11086, CVE-2019-11108, CVE-2019-11112, CVE-2019-0155, CVE-2019-11111, CVE-2019-14574, CVE-2019-14590, CVE-2019-14591, CVE-2019-11089, CVE-2019-11113, CVE-2019-0140, CVE-2019-0145, CVE-2019-0142, CVE-2019-0139, CVE-2019-0143, CVE-2019-0144, CVE-2019-0146, CVE-2019-0147, CVE-2019-0148, CVE-2019-0149, CVE-2019-0150, CVE-2019-11135, CVE-2019-11136, CVE-2019-11137, CVE-2019-11151, CVE-2019-11152, CVE-2019-11153, CVE-2019-11154, CVE-2019-11155, CVE-2019-11156, CVE-2019-14566, CVE-2019-14565, CVE-2019-11168, CVE-2019-11170, CVE-2019-11171, CVE-2019-11172, CVE-2019-11173, CVE-2019-11174, CVE-2019-11175, CVE-2019-11177, CVE-2019-11178, CVE-2019-11179, CVE-2019-11180, CVE-2019-11181 eta CVE-2019-11182.

Etiketak: Eguneraketa, Ahultasuna

SAPen 2019ko azaroko segurtasun eguneraketa

Argitalpen data: 2019/11/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa;
- SAP Diagnostic Agent (LM-Service), 7.20 bertsioa;
- SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), 4.1 eta 4.2 bertsioak;

- SAP Enable Now, 1908 baino lehenagoko bertsioak;
- S4HANA Sales (S4CORE), 1.0, 1.01, 1.02, 1.03 eta 1.04 bertsioak;
- SAP Treasury and Risk Management (EA-FINSERV), 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18 eta 8.0 bertsioak;
- SAP NetWeaver Application Server Java (J2EE-Framework), 7.1, 7.2, 7.3, 7.31, 7.4 eta 7.5 bertsioak;
- SAP Quality Management (S4CORE), 1.0, 1.01, 1.02 eta 1.03 bertsioak;
- SAP UI 700, 2.0 bertsioa;
- SAP NetWeaver AS Java, 7.10, 7.20, 7.30, 7.31, 7.4 eta 7.5 bertsioak;
- SAP Treasury and Risk Management (S4CORE), 1.01, 1.02, 1.03 eta 1.04 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 11 segurtasun ohar eta 4 eguneraketa eman ditu ezagutzera. Horietatik 4 larritasun kritikokoak dira, 1 larritasun altukoa eta 10 larritasun ertainekoak.

Argitaratutako ahultasun motak honako hauek dira:

- *SQL injection* erako ahultasun bat,
- pribilegioen eskalatze erako ahultasun bat;
- sistema eragileko komandoen injekzio erako 3 ahultasun;
- XML egiaztapen gabeziako ahultasun bat;
- baimenaren egiaztapen gabeziako ahultasun bat;
- beste era bateko ahultasun bat.

Segurtasun ohartarazpen nagusiak honi buruzkoak dira:

- Bypass anizkoitz berriak aurkitu dira Linux/Unix-erako definitutako zerrenda zurian. Hori baliatuz erasotzaile batek komando arbitrarioak ezabatu, aldatu edo exekuta litzake eragilean. Ahultasun horretarako CVE-2019-0330 identifikatzailea erabili da.
- XML baliozkotze osagarria txertatu da SAP Business Objects Business Intelligence Platform-en, iturri ez fidagarrietatik datozen XML dokumentuak ez baitziren ondo iragazten asmo gaiztoko edukia antzemateko. Hori baliatuz, erasotzaile batek informazioa heda lezake edo zerbitzuaren ukapen egoera sortu. Ahultasun horretarako CVE-2019-0396 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako honako identifikatzaileak esleitu dira: CVE-2019-0385, CVE-2019-0386, CVE-2019-0384, CVE-2019-0389, CVE-2019-0382, CVE-2019-0393, CVE-2019-0390, CVE-2019-0388, CVE-2019-0391 eta CVE-2019-0383.

Etiketak: Eguneraketa, SAP, Ahultasuna

Kodearen urruneko exekuzioa Cisco ASA eta Cisco Firepower-en (FTD)

Argitalpen data: 2019/11/13

Garrantzia: Altua

Kaltetutako baliabideak:

Cisco ASA eta Cisco FTD softwareen bertsio guztiak.

Azalpena:

Kodearen urruneko exekuzio erako ahultasun bat aurkitu da, Cisco ASA eta Cisco Firepower-en (FTD) bertsio guztietako softwarean txertatuta dagoen Lua interpretatzailearen inplementazioari eragiten diona.

Konponbidea:

Ciscok ez du argitaratu ahultasun honi aurre egiten dion software eguneraketarik. Ildo beretik, fabrikatzaileak ez du behin-behineko konponbiderik eskaini ahultasun hori une honetan arindu ahal izateko.

Ahultasun hori baliatu ahal izatearen arriskua murrizteko, INCIBE-CERTek erabiltzaileei gomendatzen die ondoko neurri babesleak hartzea:

- Cisco ASA eta Cisco Firepower (FTD) sistema edo gailu guztiei sarearen agerpena murriztea eta kanpoko sareetatik sarbiderik izan ez dezaten ziurtatzea.
- Administratzaile kredentzialekin gailuetarako sarbidea soilik konfiantzazko erabiltzaileei baimentzea, eta jatorri ezezaguneko edo fidagarriak ez diren iturrietako fitxategien exekuzioa saihestea.
- Sarean arrotzak diren erabiltzaileak antzemateko sistemak ezartzea sareko trafikoa monitorizatzeko, asmo gaiztoko jardueren bila.

Xehetasuna:

Aurkitutako ahultasunaren jatorria honakoa da: administratzaile pribilegioak dituzten erabiltzaileek erabil ditzaketen Lua scriptak baliatzearen bidez, baimendutako funtzioetara egiten diren deietan dauden murrizpen ez-nahikoak. Ahultasun hori arrakastaz baliatuz gero, erasotzaileak pilaren gainezkatze egoera aktibatu lezake eta kode arbitrarioa root pribilegioekin exekutatu, kaltetutako gailuak duen Linux sistema eragilean.

Lua scripten bitartezko Cisco ASA gailuen kasuan, administratzaile pribilegioak lituzkeen erasotzaile batek VPN saio bat ezartzeko unean dinamikoki ebaluatzen diren sarbide kontroleko atributuen kudeaketarako Dynamic Access Policy (DAP) funtzioak defini litzake.

Cisco Firepower (FTD) gailuetan Lua scriptak erabil ditzakete administratzaile pribilegioak dituzten erabiltzaileek IP trafikoa identifikatu eta iragazteko logika pertsonalizatu bat definitzeko, Firepower Management Center-en (FMC) txertatuta dagoen Custom Application Detectors funtzionaltasunaren bidez.

Etiketak: Eguneraketa, Cisco, Linux, Ahultasuna

Microsoften 2019ko azaroko segurtasun buletina

Argitalpen data: 2019/11/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows,
- Internet Explorer,
- Microsoft Edge (HTMLn oinarritutako Edge),
- ChakraCore,
- Microsoft Office eta Microsoft Office Services eta Web Apps,
- Open Source Software,
- Microsoft Exchange Server,
- Visual Studio,
- Azure Stack.

Azalpena:

Segurtasun eguneraketei buruzko Microsoften azaroko argitalpenean 75 ahultasun jaso dira, horietatik 13 kritiko gisa sailkatu dira eta 62 garrantzitsu gisa.

Konponbidea:

Dagozkien segurtasun eguneraketak instalatzea. Eguneraketen beraien instalazioari buruzko informazio orrian hori egiteko metodo ezberdinei buruzko argibideak daude.

Xehetasuna:

Argitaratutako ahultasun motak honako hauek dira:

- pribilegioak eskalatzea;
- kodearen urruneko exekuzioa;
- informazioaren zabalkundea;
- zerbitzuaren ukapena;
- ordezpena;
- segurtasun ezaugarriaren gabezia.

Etiketak: Eguneraketa, Microsoft, Nabigatzailea, Windows

Zerbitzuaren ukazio erako ahultasuna F5en BIG-IP-n

Argitalpen data: 2019/11/15

Garrantzia: Altua

Kaltetutako baliabideak:

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), 14.0.0tik 14.1.0.1era bitarteko bertsioak.

Azalpena:

TLS 1.3 aktibatuta duten BIG-IP zerbitzari birtualek zerbitzuaren ukapen egoera (DoS) jasan lezakete ezagutarazi gabeko jasotako mezuengatik.

Konponbidea:

BIG-IP ondoko bertsioetara eguneratzea:

- 15.0.0;
- 14.1.0.2.

Xehetasuna:

Ezagutarazi gabeko mezuak jasotzean ahultasun bat daukate TLS 1.3 aktibatuta duten BIG-IP zerbitzari birtualek. Urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake. Ahultasun horretarako CVE-2019-6659 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

CSV injekzio erako ahultasuna IBMren UCDn

Argitalpen data: 2019/11/15

Garrantzia: Altua

Kaltetutako baliabideak:

UCD - IBM UrbanCode Deploy.

Azalpena:

CSV injekzio erako ahultasun baten berri eman da. Hori baliatuz CSV motako asmo gaiztoko deskarga fitxategi bat sor liteke.

Konponbidea:

7.0.4.0 bertsiora edo berriagora eguneratzea.

Xehetasuna:

Bereziki diseinatutako kodea UCDan injektatuz, erasotzaile batek CSV motako asmo gaiztoko deskarga fitxategi bat sor lezake, partxeatu gabeko hirugarrenen tresnetatik irekitzean. Ahultasun horretarako CVE-2019-4490 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Moodle-n

Argitalpen data: 2019/11/18

Garrantzia: Altua

Kaltetutako baliabideak:

Ahultasunek honako bertsioei eragiten diete:

- 3.7 bertsiotik 3.7.2 bertsiora bitartekoak,
- 3.6 bertsiotik 3.6.6 bertsiora bitartekoak,
- 3.5 bertsiotik 3.5.8 bertsiora bitartekoak,
- zerbitzu teknikorik gabeko lehenagoko bertsioak.

Azalpena:

Moodle plataformari eragiten dioten sei ahultasun argitaratu dira. Larritasun altuko biak baliatuz *Cross Site Scripting* (XSS) erako erasoak egin litezke edo kontua arriskuan jarri.

Konponbidea:

3.7.3, 3.6.7 eta 3.5.9 bertsioetara eguneratzea.

Xehetasuna:

Aurkitutako sei ahultasunen artetik lau kritikotasun baxukoak dira eta beste bi kritikotasun altukoak. Horien xehetasunak honakoak dira:

- *Cross Site Scripting* (XSS) islatu erako ahultasuna akats mezu batzuetan. Ahultasun horretarako CVE-2019-14884 identifikatzailea erreserbatu da.
- OAuth 2ren saio hasiera batzuek kontuak arriskuan jar litzakete. Ahultasun horretarako CVE-2019-14880 identifikatzailea erreserbatu da.

Gainerako ahultasunetarako honako identifikatzaileak erreserbatu dira: CVE-2019-14879, CVE-2019-14881, CVE-2019-14882 eta CVE-2019-14883.

Etiketak: Eguneraketa, CMS, Ahultasuna

Ahultasuna IBMren Security Identy Manager-en

Argitalpen data: 2019/11/20

Garrantzia: Altua

Kaltetutako baliabideak:

ISIM (SS), 6.0.0 bertsioa.

Azalpena:

IBMren Security Identy Manager-ek duen ahultasun bat argitaratu da.

Konponbidea:

6.0.0.22-ISS-SIM-IF0001 bertsiora eguneratzea.

Xehetasuna:

IBM Security Identy Manager-ek duen ahultasun baten berri eman du IBMk. Ahultasun horretarako CVE-2019-4561 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM

Hainbat ahultasun IBMren Cloud Pak System-en

Argitalpen data: 2019/11/21

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Cloud Pak System, 2.3.0 bertsioa.

Azalpena:

Bi ahultasun aurkitu dira IBMren Cloud Pak System produktuan, biak larritasun altukoak.

Konponbidea:

Cloud Pak System 2.3.0.1 bertsiora eguneratzea.

Xehetasuna:

IBM Pure Application System baliatuz, sarbide lokala lukeen erabiltzaile autentifikatu batek segurtasuna saihets lezake, sarreraren baliozkotze eza dela eta. Horrela sarbidea lor lezake administratzaile pribilegioekin. Ahultasun horretarako CVE-2019-4240 identifikatzailea erreserbatu da.

IBM Pure Application System-ek kontuaren blokeatze konfigurazio okerra erabiltzen du. Hori baliatuz urruneko erasotzaile batek indar hutseko eraso bat egin lezake kontuen kredentzialak eskuratzeko. Ahultasun horretarako CVE-2019-4096 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

SQL injekzio erako ahultasuna phpMyAdmin-en

Argitalpen data: 2019/11/25

Garrantzia: Altua

Kaltetutako baliabideak:

4.9.2 baino lehenagoko phpMyAdmin-en bertsioak, gutxienez 4.7.7 bezain zaharrak direnak.

Azalpena:

phpMyAdmin-en ekipoko William Desportes-ek SQL injekzio erako ahultasun bat aurkitu du.

Konponbidea:

4.9.2 edo goragoko bertsiora eguneratzea edo dagokion partxea aplikatzea.

Xehetasuna:

Ezagutzera eman den ahultasun baten arabera, datu base baten izen bat erabil liteke, bereziki diseinatua, SQL injekzio erako eraso bat egiteko, editoreak duen funtzionaltasun baten bidez. Ahultasun horretarako CVE-2019-18622 identifikatzailea erabili da.

Etiketak: Eguneraketa, PHP, Ahultasuna

Autentifikazioaren saiheste erako ahultasuna F5en BIG-IPn

Argitalpen data: 2019/11/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), honako bertsio hauek:

- 15.x:
  - 15.0.1.0.33.11-ENG Hotfix;
  - 15.0.1.0.48.11-ENG Hotfix.
- 14.x:
  - 14.1.0.3.0.79.6-ENG Hotfix;
  - 14.1.0.3.0.97.6-ENG Hotfix;
  - 14.1.0.3.0.99.6-ENG Hotfix;
  - 14.1.0.5.0.15.5-ENG Hotfix;
  - 14.1.0.5.0.36.5-ENG Hotfix;
  - 14.1.0.5.0.40.5-ENG Hotfix;
  - 14.1.0.6.0.11.9-ENG Hotfix;
  - 14.1.0.6.0.14.9-ENG Hotfix;
  - 14.1.0.6.0.68.9-ENG Hotfix;
  - 14.1.0.6.0.70.9-ENG Hotfix;
  - 14.1.2.0.11.37-ENG Hotfix;
  - 14.1.2.0.18.37-ENG Hotfix;
  - 14.1.2.0.32.37-ENG Hotfix;
  - 14.1.2.1.0.46.4-ENG Hotfix;
  - 14.1.2.1.0.14.4-ENG Hotfix;
  - 14.1.2.1.0.16.4-ENG Hotfix;
  - 14.1.2.1.0.34.4-ENG Hotfix;
  - 14.1.2.1.0.97.4-ENG Hotfix;
  - 14.1.2.1.0.99.4-ENG Hotfix;
  - 14.1.2.1.0.105.4-ENG Hotfix;
  - 14.1.2.1.0.111.4-ENG Hotfix;
  - 14.1.2.1.0.115.4-ENG Hotfix;
  - 14.1.2.1.0.122.4-ENG Hotfix.

OHARRA: ahultasun honek soilik eragiten die F5en zerbitzutik eskuratutako BIG-IP Engineering-en *hotfix*-ei.F5en deskargen webgunetik

eskuratutako *major*, *minor* edo *maintenance* bertsioak ez daude kaltetuak.

Azalpena:

Hainbat zerbitzarirekin kudeaketaren autentifikazioa egiteko Active Directory, LDAP edo Client Certificate LDAPek erabiltzen duten BIG-IP konfigurazioei eragin diezaieke ahultasun honek. Hori baliatuz autentifikazioa saihets liteke eta ondorioz sistema osorik jar liteke arriskutan.

Konponbidea:

Ahultasun hau konpontzeko ez dago eguneraketarik eskuragarri. Ahultasuna arintzeko, F5ek ondoko neurriak hartzea gomendatzen du:

- Urruneko edozein LDAP autentifikazio desgaitzea urruneko erabiltzaileentzat.
- Urruneko LDAP autentifikazioa konfiguratzea autentifikazio zerbitzari bakarrarekin.
- BIG-IP sistemaren kudeaketa interfazearen jatorriko IP helbidean oinarritutako sarbide kontrol zorrotzak ezartzea.

Xehetasuna:

BIG-IP sisteman LDAP, Active Directory edo Client Certificate LDAP erabiliz autentifikatzen diren urruneko erabiltzaileek kredentzial okerrekin has dezakete saioa, eta horrela osorik jar dezakete arriskuan BIG-IP sistema. Ahultasun horretarako CVE-2019-6675 identifikatzailea erreserbatu da.

Etiketak: Ahultasuna

Hainbat ahultasun F5 produktuetan

Argitalpen data: 2019/11/27

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;
  - 14.1.0 - 14.1.2;
  - 14.0.0 - 14.0.1;
  - 13.1.0 - 13.1.3.1;
  - 12.1.0 - 12.1.5;
  - 11.5.1 - 11.6.5.
- Enterprise Manager, 3.1.1 bertsioa.
- BIG-IQ Centralized Management, honako bertsioak:
  - 6.0.0;
  - 5.2.0 - 5.4.0.
- F5 iWorkflow 2.3.0 bertsioa.

Azalpena:

F5 produktuek dituzten hainbat ahultasunen berri eman da. Horiek baliatuz erasotzaile batek proxy-a konfigura lezake trafikoa gelditzeko, zerbitzua ukatzeko edo *root* kontuaren fitxategietara sarbidea lortzeko.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), honako bertsio hauek:
  - 15.0.1.1;
  - 14.1.2.1;
  - 14.0.1.1;
  - 13.1.3.2;
  - 12.1.5;
  - 11.6.5.1;
- BIG-IQ Centralized Management, 6.1.00 bertsioa.

Xehetasuna:

- Autentifikazio token-era sarbidea izanez gero, erasotzailea BIG-IP ASM Central Policy Builder balitz bezala joka lezake eta iradokizun datu hondatuak edo okerrak bidal litzake BIG-IQ/Enterprise Manager/F5 iWorkflow-era. Horren ondorioz politikak prestatzeko iradokizun okerrak eman litezke, edo zerbitzuaren ukapen egoera (DoS) partziala eragin liteke. Ahultasun horretarako CVE-2019-6665 identifikatzailea erreserbatu da.
- Traffic Management Microkernel-en (TMM) berrabiatze baten ondoren suspertzen denean aldi batez akatsa ematen du trafikoa prozesatzean, eta gailu multzo batean konfiguratutako gailuek ere akatsa eman dezakete. Ahultasun horretarako CVE-2019-6666 eta CVE-2019-6667 identifikatzaileak erreserbatu dira.
- BIG-IP Edge Client-ek ahalbidetu lezake kaltetutako macOS gailuan pribilegiorik ez duen erasotzaile batek bezero lokalaren host-ean root kontukoak diren fitxategien jabetza eskuratzea. Ahultasun horretarako CVE-2019-6668 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna