2020ko Uztailaren Bulletina

Ohartarazpenak - Teknikoak

Kodearen urrutiko exekuzioaren ahultasuna F5 erakundearen TMUI sisteman

Argitalpen data: 2020/07/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), bertsioak:

- 15.1.0 eta 15.0.0;
- 14.1.0tik 14.1.2ra;
- 13.1.0tik 13.1.3ra;
- 12.1.0tik 12.1.5era;
- 11.6.1etik 11.6.5era;

Azalpena:

Positive Technologies enpresako Mikhail Klyuchnikov ikertzaileak F5 erakundeari larritasun kritikoko ahultasun baten eman zion; kodearen urrutiko exekutatze motakoa da, eta TMUI (Traffic Management User Interface) sistemari eragiten dio.

Konponbidea:

Kaltetutako produktuak honako bertsioren batera eguneratzea:

- 15.1.0.4;
- 14.1.2.6;
- 13.1.3.4;
- 12.1.5.2;
- 11.6.5.2.

Xehetasuna:

Ahultasun horren bidez, TMUI sarerako sarbidea duen erasotzaile batek (konfigurazio erabilera gisa ere ezaguna), Self IPs edota BIG-IP administrazio portuaren bidez, sistemaren komando arbitrarioak exekuta litzake, artxiboak sortu edo ezabatu, zerbitzuak desgaitu edota Java kodea modu arbitrarioaren exekutatu. Horrek, sistema osoa konprometitu lezake. Ahultasun horretarako, CVE-2020-5902 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

RCE ahultasunak Microsoft Windows Codecs Library sisteman

Argitalpen data: 2020/07/02

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Microsoft Windows Codecs Library sistema, Windows 10 bertsio ezberdinetan, soilik Microsoft Store dendako aukerako HEVC

multimedia codec-ak instalatu dituzten bezeroak (gailuaren fabrikatzaileak barne).

Azalpena:

Zero Day Initiative de Trend Micro ekimeneko Abdul-Aziz Hariri ikertzaileak bi ahultasunen berri eman dio Microsoft etxeari. Bata larritasun kritikokoa eta beste larritasun handikoa, biak urruneko kode exekuzio motakoak (RCE). Microsoft Windows Codecs Library sistemari eragiten diote.

Konponbidea:

Ahultasun horiek konpontzen dituzten bertsioak honakoak dira: 1.0.31822.0, 1.0.31823.0 eta ostekoak.

Kaltetutako bezeroak Microsoft Storek eguneratuko ditu zuzenean, eta ez dute ezer egin beharrik eguneratzea jasotzeko, soilik eguneratze automatikoen funtzionalitatea aktibatuta dutela ziurtatu.

Bestela, eguneratzea berehala jaso nahi duten bezeroek Microsoft Store aplikazioarekin bila ditzakete eguneratzeak.

Xehetasuna:

- Kodearen urrutiko exekutatzearen arloko ahultasun bat dago (RCE) Microsoft Windows Codecs Library sistemak memorian objektuak kudeatzeko daukan moduan. Ahultasun hori baliatzeko, programa batek bereziki diseinatutako irudi-artxibo bat prozesatu behar du. Erasotzaile batek erabiltzailearen sistema are gehiago konprometitzeko informazioa lortu lezake. Ahultasun horretarako, CVE-2020-1425 identifikatzailea erreserbatu da.
- Kodearen urrutiko exekutatzearen arloko ahultasun bat dago (RCE) Microsoft Windows Codecs Library sistemak memorian objektuak kudeatzeko daukan moduan, eta erasotzaile batek kode arbitrarioa exekutatu lezake. Ahultasun hori baliatzeko, programa batek bereziki diseinatutako irudi-artxibo bat prozesatu behar du. Ahultasun horretarako, CVE-2020-1457 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Microsoft, Ahultasuna, Windows.

Hainbat ahultasun Citrix produktu batzuetan

Argitalpen data: 2020/07/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Citrix ADC eta Citrix Gateway, 13.0-58.30 bertsioaren aurrekoak;
- Citrix ADC eta Citrix Gateway, 12.1-57.18 bertsioaren aurrekoak;
- Citrix ADC eta Citrix Gateway, 12.0-63.21 bertsioaren aurrekoak;
- Citrix ADC eta Citrix Gateway, 11.1-64.14 bertsioaren aurrekoak;
- NetScaler ADC eta NetScaler Gateway, 10.5-70.18 bertsioaren aurrekoak;
- Citrix SD-WAN WANOP, 11.1.1ay bertsioaren aurrekoak;
- Citrix SD-WAN WANOP, 11.0.3d bertsioaren aurrekoak;
- Citrix SD-WAN WANOP, 10.2.7 bertsioaren aurrekoak;
- Linuxerako Citrix Gateway Plug-in, 1.0.0.137 bertsioaren aurrekoak.

Azalpena:

Citrix erakundeak Citrix ADC? (NetScaler ADC izenez ezagunak), Citrix Gateway?(NetScaler Gateway gisa ezagunak) eta Citrix SD-WAN WANOP produktuen ahultasunen berri eman du. Horiek baliatuta, erasotzaile batek zerbitzu ukapena eragin lezake, baita kode injekzioak, pribilegioen igoera, informazioaren zabalkundea edota Cross Site Scripting (XSS) ere.

Konponbidea:

Citrixek Citrix ADC, Citrix Gateway eta Citrix SD-WAN WANOP produktuetarako bertsioak kaleratu ditu, ahultasun horiek konpontzeko. Citrixek gomendatu du bezeroek instalazio horiek berehala instalatzeko.

Xehetasuna:

Citrix erakundeak jakinarazitako ahultasunen bidez, kaltetutako sistemak konprometitu daitezke, administrazio interfazean Cross Site Scripting (XSS) eraso bat burutu edo gailurako deskarga bat egin; horrela, erabiltzailearen ekipo lokala konprometitu daiteke administrazio saretik eginez gero, baita zerbitzu ukapena eragin edota pribilegioetan gora egin ere.

Ahultasun horietarako, honako identifikatzaileak erreserbatu dira: CVE-2019-18177, CVE-2020-8187, CVE-2020-8190, CVE-2020-8191, CVE-2020-8193, CVE-2020-8194, CVE-2020-8195, CVE-2020-8196, CVE-2020-8197, CVE-2020-8198 eta CVE-2020-8199.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Xen sisteman

Argitalpen data: 2020/07/08

Garrantzia: Handia

Kaltetutako baliabideak:

Xen tresnaren bertsio guztiak dira ahulak.

Azalpena:

Hainbat ikertzailek 5 ahultasun atzeman dituzte, eta Xen tresnaren bertsio guztiei eragiten diete.

Konponbidea:

Xen tresnaren abisu bakoitzaren *RESOLUTION* atalean zerrendatuta agertzen diren partxeak aplikatzea. *Erreferentziak* atalean daude eskuragarri.

Xehetasuna:

- Administraria gonbidatu (guest) gisa agertzen denean, 1023 ekitaldi kanal baino baimentzeko, gonbidatu horrek host delakoa blokeatu dezake. Xen memoriarik gabe geratzen denean, ekitaldien kanal berrien esleipenak host delakoa blokeatzea eragingo du, errore gisa informatu beharrean. Ahultasun horretarako, CVE-2020-15566 identifikatzailea esleitu da.
- Asmo txarreko HVM gonbidatu batek eragin lezake hipervisor tresna blokeatzea. Ondorioz, zerbitzu ukapena eragin dezake (DoS), eta host osoari eragingo lioke. Ahultasun horretarako, CVE-2020-15563 identifikatzailea esleitu da.
- Asmo txarreko gonbidatu batek DMA idazketa/irakurketa sarbidea izan lezake Xen tresnaren pool delakora itzulitako frameei dagokienez, eta gero beste helburu baterako berrerabili. Horrela, host delakoa blokeatu liteke (eta horren zerbitzu ukapena eragingo luke), eta pribilegioak handitzeko aukera eman. Ahultasun horretarako, CVE-2020-15565 identifikatzailea esleitu da.
- Administrari gonbidatu batek, asmo txarrez, hipervisor tresna blokeatu lezake, eta horrek zerbitzu ukapena ekarriko luke (DoS). Ahultasun horretarako, CVE-2020-15564 identifikatzailea esleitu da.
- Administrari gonbidatu batek, edota pribilegiorik gabeko erabiltzaile gonbidatu batek, zerbitzu ukapena eragin lezake, datuen ustelkeria edota pribilegioen handitzea. Ahultasun horretarako, CVE-2020-15567 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Juniper etxearen Junos Space eta Junos OS tresnetan

Argitalpen data: 2020/07/09

Garantzia: Kritikoa

Kaltetutako baliabideak:

- SRX Series plataformako Junos OS, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2 eta 19.3 bertsioak;
- Junos Space-ren Junos Space Security Director, 20.1R1 bertsioaren aurrekoak.

Azalpena:

Juniper etxeak jakinarazi du hainbat ahultasun daudela Junos OS eta Junos Space Security Director produktuetan. Horiek baliatuta, erasotzaile batek urrutiko kodea exekutatu lezake sistemetan, edo zerbitzu ukapena eragin.

Konponbidea:

- Junos OS bertsio hauetara eguneratzea: 18.1R3-S9, 18.2R2-S7, 18.2R3-S3, 18.3R1-S7, 18.3R2-S4, 18.3R3-S1, 18.4R1-S7, 18.4R2 -S4, 18.4R3, 19.1R1-S5, 19.1R2, 19.2R1-S2, 19.2R2, 19.3R2 edo 19.4R1;
- Junos Space Security Director 20.1R1 bertsiora eguneratzea.

Xehetasuna:

Junos OS tresnan atzemandako ahultasunak ICAP birbideratze zerbitzuan ematen dira, HTTP mezu baten prozesatzen desegokiaren bidez, edo memoriaren datuen kudeaketa okerraren bidez. Ahultasun horiek kritikotzat jo dira, eta ICAP zerbitzua egokituta dagoenean soilik dira eraginkorrak.

Junos Space Security Director produktuaren ahultasunei dagokienez, Juniperrek 105 ahultasun zuzendu ditu guztira, 20.1R1 bertsioan. Horietako 18 kritikoak izan dira.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna

IBM Verify Gatewayn baimendu gabeko APIrako deien aurkako babes nahikorik ez izatea

Argitalepen data: 2020/07/24

Garrantzia: Altua

Kaltetutako baliabideak:

- IBM Verify Gateway (IVG) RADIUS 1.0.0;
- IBM Verify Gateway (IVG) PAM 1.0.0, 1.0.1;
- IBM Verify Gateway (IVG) WinLogin 1.0.0, 1.0.1.

Azalpena:

IBM Verify Gatewayn baimendu gabeko APIrako deien aurkako babes nahikorik ez izateak erasotzaile bati ahalbidetuko lioke sartzeko token bat lortzea eta helburu maltzurrekin erabiltzea.

Konponbidea:

Eguneratu bertsio hauetara:

- IBM Security Verify Gateway, AIX PAM-erako (Pluggable Authentication Modules) v1.0.1;
- IBM Security Verify Gateway Linux PAM-erako (Pluggable Authentication Modules) v1.0.2;
- IBM Security Verify Gateway RADIUSerako v1.0.1;
- IBM Security Verify Gateway Windows Login-erako v1.0.2.

Xehetasuna:

IBM Verify Gatewayren (IVG) osagaiek APIrako deiak egiten dituztenean, ez dago behar adina babes. Horri esker, erasotzaile batek sartzeko beste token batzuk lor ditzake, eta APIrako beste dei batean erabili, ordezkatze bat eginez.

Etiketak: Eguneraketa, IBM, Ahultasuna

Direktorio mugatu baterako mugatze ez zuzena Dell EMC OMSA sisteman

Argitalpen data: 2020/07/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Dell EMC OpenManage Server Administrator (OMSA), 9.4 bertsioa eta aurrekoak.

Azalpena:

Rhino Security Labs enpresako David Yesland ikertzaileak larritasun kritikoko ahultasun baten berri eman dio Dell EMC erakundeari. Direktorio mugatu baterako ibilbidearen izenaren mugatze desegokiari dagokio (*path traversal*), eta OpenManage Server Administrator (OMSA) produktuari eragiten dio.

Konponbidea:

Dell EMC OpenManage Server Administrator (OMSA) 9.3.0.2 edo 9.4.0.2 bertsioetara eguneratzea.

Xehetasunak:

Egiaztatu gabeko urrutiko erasotzaile batek ahultasun hori baliatu lezake webgunera bereziki diseinatutako API eskaera bat bidalita, konprometitutako administrazio estazioan artxiboen sistemarako sarbidea lortzeko. Ahultasun horretarako, CVE-2020-5377 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2020/07/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- *.ova* edo *.iso* motako artxiboak erabiliz instalatu ziren Cisco DCNM gailu guztien inplementazio moduak;
- Cisco DCNM, 11.0(1), 11.1(1), 11.2(1) eta 11.3(1) bertsioak;
- Cisco SD-WAN vManage Cisco bertsio ahul bat exekutatzen ari diren Cisco gailu guztiak;
- Cisco SD-WAN Solution Software sistemaren bertsio ahul bat exekutatzen ari diren honako produktuak:
  - IOS XE SD-WAN Software,
  - SD-WAN vBond Orchestrator Software,
  - SD-WAN vEdge Cloud Routers,
  - SD-WAN vEdge Routers,
  - SD-WAN vManage Software,
  - SD-WAN vSmart Controller Software.

Azalpena:

Cisco produktu batzuei eragiten dieten 3 ahultasun atzeman ditu, larritasun kritikokoak.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneratzeak Ciscoren Software deskarga panelean deskargatu daitezke: Informazio zehatzagoa izateko, kontsultatu *Erreferentzien atala.*

Xehetasunak:

- Cisco Data Center Network Manager (DCNM) sistemaren API REST ataleko ahultasun baten ondorioz, urrutiko erasotzaile batek egiaztatzea alde batera utzi eta administrari pribilegioak behar dituen ekintza arbitrarioak burutu litzake kaltetutako gailuan. Ahultasun horretarako, CVE-2020-3382 identifikatzailea erreserbatu da.
- Cisco SD-WAN vManage softwarearen administrazio webgunearen interfazearen ahultasun baten ondorioz, urrutiko

erasotzaile batek, egiaztatuta, baimena alde batera utzi eta informazio konfidentziala eskuratu lezake, sistemaren konfigurazioa aldatu edo kaltetutako gailuaren eskuragarritasunean eragin. Ahultasun horretarako, CVE-2020-3374 identifikatzailea erreserbatu da.
- Cisco SD-WAN Solution Software sistemaren ahultasun baten ondorioz, egiaztatu gabeko urrutiko erasotzaile batek kaltetutako gailuan bufferrak gainezka egitea eragin lezake. Ahultasun horretarako, CVE-2020-3375 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Cisco, Ahultasuna

GRUB2 eta UEFI Secure Boot sistemen ahultasunak

Argitalpen data: 2020/07/30

Garrantzia: Handia

Kaltetutako baliabideak:

GRUB2 erabiltzen duten sistemak daude ahultasun horren mende.

Azalpena:

Eclypsium enpresako segurtasun-ikertzaileek bufferraren gainezkatze arloko ahultasun bat aurkitu dute GRUB2 sisteman. *BootHole* dauka izena, eta, horren bidez, erasotzaile batek sisteman iraun dezake eta abiarazte-prozesua kontrolatu, sistema eragilea bera kargatu baino lehen.

Konponbidea:

Bootloader delakoa edo GRUB2 abiarazte-kargagailua azken bertsiora eguneratzea. Linux banaketek bakoitzerako hainbat partxe argitaratu dituzte.

Beste fabrikatzaile batzuek ziurtagiri baliodunen (db) eta ezeztatuen (dbx) datu-baseak eta Microsoftek erabiltzen duen *Secure Boot* sistemarako CA erabiltzen duten abiarazte-kargagailuak eta *Shim* eguneratu beharko dituzte (auto-sinatutako CA ziurtagiria txertatzen duen lehen etapako abiarazte-kargagailua).

Erreferentzien atala kontsulta daiteke fabrikatzaileen eguneratzeei buruzko informazio gehiago lortzeko.

Xehetasunak:

Atzemandako ahultasuna GRUB2 sisteman bufferraren gainezkatzea gertatzearen ondorioz sortzen da, baita *Secure Boot* aukera aktibatuta dagoenean ere. Gainezka egitea *grub.cfg* testu fitxategi baten bidez gertatzen da. Komandoen sekuentzia abiaraztean zehar gertatzen da, eta kaltetutako sistemetan administrari baimenekin aldatu daiteke.

Sistemaren administrari baimenak dituen erasotzaile batek grub.cfg fitxategia alda dezake, eta, horrela, sistemaren abiarazte-prozesurako sarbidea izango luke, sistema eragilea kargatu aurretik.

Atzemandako akatsaren bidez, UEFI abiarazteetan firmware sinadurarako eskuragarri dauden *Secure Boot* aukerak eta fabrikatzaileen *Shim* erabilera alde batera utz daitezke; horrela izanik, baliogabetu egiten da Secure Boot bidez UEFI sistemetan hirugarrenen abiarazte kargagailuak edo *bootloader* delakoak baimentzen dituen konfiantzazko CA sistema, Windowsek kudeatzen duena.

BootHole ahultasun horrek CVE-2020-10713 identifikatzailea dauka esleituta.

Gainera, Eclypsium erakundeak larritasun txikiagoko beste ahultasun batzuk aurkitu ditu GRUB2 sisteman, honako identifikatzaileekin: CVE-2020-14308, CVE-2020-14309, CVE-2020-14310, CVE-2020-14311, CVE-2020-15705, CVE-2020-15706 eta CVE- 2020-15707.

Etiketak: Eguneratzea, HP, Linux, Microsoft, VMware, Ahultasuna, Windows