2021ko Otsailaren Bulletina

Ohartarazpenak - Teknikoak

HPE Moonshot Provisioning Manager sisteman direktorio mugaturako muga desegokia

Argitalpen data: 2021/02/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HPE Moonshot Provisioning Manager, 1.20 bertsioa.

Azalpena:

Erik de Jong ikertzaileak, Trend Microko ZDIren laguntzarekin, ahultasun baten berri eman dio HPEri. Larritasun kritikokoa da, direktorio mugaturako sarbide desegokiaren motakoa (*directory traversal*).

Konponbidea:

KoHPEren gomendioa da bezeroek Moonshot Provisioning Manager sistema erabiltzeari uztea. HPE Moonshot Provisioning Manager aplikazioa deskatalogatua dago, ez du laguntzarik jasotzen, ez dago deskargatzeko eskuragarri HPEren laguntza zentroan, eta ez dago partxerik eskuragarri.

Xehetasuna:

Ahultasuna urrutiko erasotzaile batek baliatu lezake, egiaztatu gabe, direktorio mugatuaren mugatze desegokia eragiteko (*directory traversal*) erabiltzaileak emandako khuploadfile.cgi sarbidean; izan ere, erabiltzailea balioztatzeko segurtasun nahikorik ez dago, eta kontrolik gabe sar liteke edozein direktoriotara; horrela izanik, kodearen urrutiko exekuzioa eragin liteke, zerbitzu ukapena, edota sistemaren integritatea konprometitu liteke. Ahultasun horretarako, CVE-2021-25140 identifikatzailea esleitu da.

Etiketak: HP, Ahultasuna

Kode injekzioa IBM Spectrum Protect produktuetan

Argitalpen data: 2021/02/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Virtual Environments eremurako IBM Spectrum Protect: VMware eremurako Data Protection, bertsioak: 8.1.0.0-8.1.10.0 eta 7.1.0.0-7.1.8.9;
- Virtual Environments eremurako IBM Spectrum Protect: Hyper-V eremurako Data Protection, bertsioak: 8.1.0.0-8.1.10.0;
- VMware eremurako IBM Spectrum Protect Snapshot, bertsioak: 4.1.0.0-4.1.6.10.

Azalpena:

IBM Spectrum Protect produktuetan esportazioaren aurreko datuen balioztatze desegokia eginez gero, erasotzaile batek kode arbitrarioa exekuta lezake sisteman.

Konponbidea:

- Virtual Environments eremurako IBM Spectrum Protect: VMware Release eremurako Data Protection:
  - 8.1 bertsioa: 8.1.11 bertsiora eguneratzea;
  - 7.1 bertsioa: 7.1.8.10 bertsiora eguneratzea;
- Virtual Environments eremurako IBM Spectrum Protect: Hyper-V Release eremurako Data Protection:
  - 8.1 bertsioa: 8.1.11 bertsiora eguneratzea;
- VMware Release eremurako IBM Spectrum Protect Snapshot:
  - 4.1 bertsioa: 4.1.6.11 bertsiora eguneratzea;

Xehetasuna:

Esportazioaren aurreko datuen balioztatze desegokia eginez gero, erasotzaile batek kode arbitrarioa exekuta lezake sisteman. Ahultasun horretarako, CVE-2020-4693 identifikatzailea esleitu da.

Etiketak: Eguneratzea, IBM, Ahultasuna

Zerbitzu ukapena Allen-Bradleyren Flex IO 1794-AENT/B sisteman

Argitalpen data: 2021/02/03

Garrantzia: Handia

Kaltetutako baliabideak:

Flex IO 1794-AENT/B, 4.003 bertsioa.

Azalpena:

Cisco Talos erakundeko Jared Rittle ikertzaileak jakinarazi du larritasun handiko ahultasun bat dagoela. Horren bidez, erasotzaile batek zerbitzu ukapena eragin lezake (DoS).

Konponbidea:

Gaur egun, ez dago eguneratzerik eskuragarri.

Xehetasuna:

Bufferraren gainezkatze motako ahultasun baten bidez, ENIP eskaera-ibilbidearen sareko segmentuaren funtzionalitatean, erasotzaile batek zerbitzu ukapena eragin lezake, bereziki diseinatutako sare-eskaera bidaliz. Ahultasun horretarako CVE 2020-6088 identifikatzailea esleitu da.

Etiketak: 0day, Komunikazioak, Ahultasuna

Hainbat ahultasun Cisco Small Business VPN Routers sistemetan

Argitalpen data: 2021/02/04

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Ahultasun horiek Cisco Small Business *router* hauei eragiten die, 1.0.01.02 bertsioaren aurreko *firmware* bertsio bat exekutatzen badute:

- RV160 VPN Router,
- RV160W Wireless-AC VPN Router,
- RV260 VPN Router,
- RV260P VPN Router con POE,
- RV260W Wireless-AC VPN Router.

Azalpena:

Hainbat ikertzaileak 7 ahultasunen berri eman diote Cisco erakundeari. Guztiak dira larritasun kritikokoak, eta kaltetutako produktuen kudeaketa webgunearen interfazeari eragiten diote.

Konponbidea:

Ciscok ahultasun horiek konpondu ditu Cisco RV160, RV160W, RV260, RV260P eta RV260W routerretarako 1.0.01.02 eta osteko firmware bertsioetan. Eskuragarri Ciscoren software deskarga panelean.

Xehetasuna:

HTTP eskaerak oker balioztatuta, urrutiko erasotzaile batek, egiaztatu beharrik gabe, kode arbitrarioa exekuta lezake root gisa kaltetutako gailuan, webguneko administrazio interfazera bereziki diseinatutako HTTP eskaerak bidaliz. Ahultasun horietarako CVE-2021-1289, CVE-2021-1290, CVE-2021-1291, CVE-2021-1292, CVE-2021-1293, CVE-2021-1294 eta CVE-2021-1295 identifikatzaileak esleitu dira.

Etiketak: Eguneratzea, Cisco, Komunikazioak, Ahultasuna.

Hainbat ahultasun SolarWinds Orion Platform sisteman

Argitalpen data: 2021/02/05

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Orion Platform, 2020.2.4 bertsioaren aurrekoak;
- ServU-FTP, 15.2.2 Hotfix 1 bertsioaren aurrekoak.

Azalpena:

Martin Rakhmanov, Trustwave erakundeko ikertzaileak artikulu bat argitaratu du. Horren bidez, 3 ahultasun kritiko azaldu ditu. SolarWinds Orion User Device Tracker eta SolarWinds Serv-U FTP sistemei eragiten diete. Ahultasun horien bidez, erasotzaile batek kodearen urrutiko exekuzioa burutu lezake, edo kredentzialetara sartu liteke sistemako edozein artxibo berreskuratu, irakurri, editatu edota ezabatzeko.

Konponbidea:

Zuzenketak SolarWinds produktuen honako bertsioetan daude eskuragarri:

- Orion Platform 2020.2.4;
- ServU-FTP 15.2.2 Hotfix 1.

Xehetasuna:

- SolarWinds Orion Collector zerbitzua MSMQ (Microsoft Message Queue) delakoaren mende dago, neurri handi batean. Lerro pribatu ugari daude eskuragarri, denak egiaztatu gabe. Horrek esan nahi du egiaztatu gabeko erabiltzaileek mezuak bidali ditzaketela lerroetara TCP 1801 portuaren bidez. Deserializazio ez seguru bat dela eta, pribilegiorik gabeko erabiltzaile batek kode arbitrarioa urrunetik exekuta lezake. Ahultasun horretarako, CVE-2021-25274 identifikatzailea esleitu da.
- Orion sistemaren *backend* delakoaren datuen oinarriaren kredentzialak ez zeuden behar bezala babestuta, eta tokiko erabiltzaileek murrizketarik gabeko sarbidea egin zezaketen horietara. Erasotzaile batek egoera hori baliatu lezake SolarWinds Orion sistemaren datu-basea kontrolatzeko eta informazioa lapurtu edo administrari mailan erabiltzaileak gehitzeko. Ahultasun horretarako, CVE-2021-25275 identifikatzailea esleitu da.
- SolarWinds Serv-U FTP Server zerbitzarian kokatutako kontuak diskoan banatutako artxiboetan gordetzen dira, eta egiaztatutako erabiltzaile batek horietarako sarbidea dauka. FTP zerbitzaria *LocalSystem* baimenen bidez exekutatzen da, beraz, administrari kontu bat sortzean, erasotzaile batek hasierako direktorioa ezarri lezake sistemaren unitatearen erroan, eta, horrela, edozein artxibo irakurri edo ordeztu lezake. Ahultasun horretarako, CVE-2021-25276 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Azpiegitura kritikoak, Birtualizazioa, Ahultasuna.

Hainbat ahultasun Dell PowerScale OneFS sisteman

Argitalpen data: 2021/02/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Dell PowerScale OneFS, bertsioak:

- 8.1.0;
- 8.1.1;
- 8.1.2;
- 8.2.0;
- 8.2.1;
- 8.2.2;
- 9.0.0;
- 9.1.0

Azalpena:

Dell EMC erakundeak 7 ahultasun antzeman ditu; bat larritasun kritikokoa da, 4 handikoak eta 2 tarteko larritasunekoak. Horien bidez, erasotzaileek PowerScale OneFS sistema konprometitu lezakete.

Konponbidea:

PowerScale deskarga gunearen bidez, fabrikatzailearen oharreko Affected Products and Remediation atalean kaltetutako bertsio bakoitzerako azaldutako ekintza zehatzak burutzea.

Xehetasuna:

Dell PowerScale OneFS sistemak kontua iraungi osteko SSH gakoaren erabileraren motako ahultasun bat dauka. *ISI_PRIV_AUTH_SSH* eremuan RBAC pribilegioa daukan sareko erabiltzaile batek (*Role-Based Access Control*), kontua iraungita

badauka, ahultasun hori baliatu lezake kontua iraungi aurretik zeukan sarbidea lortuz. Gainera, baliteke kontuak pribilegio handiak izatea. Ahultasun kritiko horretarako, CVE-2021-21502 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak esleitu dira: CVE-2020-26191, CVE-2020-26192, CVE-2020-26195, CVE-2020-26194, CVE-2020-26195 eta CVE-2020-26196.

Etiketak: Eguneratzea, Ahultasuna

Microsoften segurtasun-eguneratzeak. 2021eko otsaila.

Argitalpen data: 2021/02/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- . NET Core;
- .NET Framework;
- Azure IoT;
- Developer Tools;
- Microsoft Azure Kubernetes Service;
- Microsoft Dynamics;
- Microsoft Edge Android-erako;
- Microsoft Exchange Server;
- Microsoft Graphics Component;
- Microsoft Office Excel;
- Microsoft Office SharePoint;
- Microsoft Windows Codecs Library;
- Role: DNS Server;
- Role: Hyper-V;
- Role: Windows Fax Service;
- Business-erako Skype;
- SysInternals;
- System Center;
- Visual Studio;
- Windows Address Book;
- Windows Backup Engine;
- Windows Console Driver;
- Windows Defender;
- Windows DirectX;
- Windows Event Tracing;
- Windows Installer;
- Windows Kernel;
- Windows Mobile Device Management;
- Windows Network File System;
- Windows PFX Encryption;
- Windows PKU2U;
- Windows PowerShell;
- Windows Print Spooler Components;
- Windows Remote Procedure Call;
- Windows TCP/IP;
- Windows Trust Verification API.

Azalpena:

Segurtasun eguneratzeen inguruko Microsoft argitalpenean 65 ahultasun jaso dira; 11 kritiko gisa sailkatu dira, 45 garrantzitsu gisa, 2 moderatu gisa eta 7 oraindik larritasun-mailarik esleitu gabe.

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 ezaugarrien omisioa,
- Nortasuna ordeztea (spoofing).

GARRANTZITSUA

- Microsoftek segurtasun-ohar bat argitaratu du larritasun handiko ahultasun bat konpontzeko, Microsoft Wink32k sistemako pribilegioen eskalatzearen motakoa, CVE-2021-1732 identifikatzailearekin.
- Tokiko erasotzaile batek ahultasun hori baliatu lezake kaltetutako sistema baten kontrola bereganatzeko. Ahultasun hori egun baliatzen ari dira.
- Microsoftek post argitaratu du, eta horren bidez adierazi du 3 ahultasun daudela Windowsen TCP/IP inplementazioan, eta erasotzaileek urrunetik baliatu ditzaketela, egiaztatu beharrik gabe. Lehenengo biak larritasun kritikokoak dira, eta horien bidez urrutiko kodea exekutatu liteke (CVE-2021-24074 eta CVE-2021-24094); hirugarrena larritasun handikoa

da, eta horren bidez zerbitzu ukapenaren motako erasoak burutu litezke (CVE-2021-24086).

Etiketak: 0day, Eguneratzea, Komunikazioak, DNS, IoT, Microsoft, Nabigatzailea, Pribatutasuna, Ahultasuna.

2021eko otsaileko SAP segurtasun-eguneratzea

Argitalpen data: 2021/02/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa;
- SAP Commerce, 1808, 1811, 1905, 2005 eta 2011 bertsioak;
- SAP Business Warehouse, bertsioak: 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755 eta 782;
- SAP NetWeaver AS ABAP (SAP Landscape Transformation - DMIS), bertsioak: 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731 eta 2011_1_752, 2020;
- SAP S4 HANA (SAP Landscape Transformation), bertsioak: 101, 102, 103, 104 eta 105;
- SAP NetWeaver AS ABAP, bertsioak: 740, 750, 751, 752, 753, 754 eta 755;
- SAP Software Provisioning Manager 1.0 (SAP NetWeaver Master Data Management Server 7.1), 1.0 bertsioa;
- SAP NetWeaver Process Integration (Java Proxy Runtime), bertsioak: 7.10, 7.11, 7.30, 7.31, 7.40 eta 7.50;
- SAP Business Objects Business Intelligence Platform (CMC and BI Launchpad), bertsioak: 410, 420 eta 430;
- SAP UI5, bertsioak: 1.38.49, 1.52.49, 1.60.34, 1.71.31, 1.78.18, 1.84.5, 1.85.4 eta 1.86.1;
- SAP Web Dynpro ABAP;
- SAP UI, bertsioak: 7.5, 7.51, 7.52, 7.53 eta 7.54;
- SAP UI 700, 2.0 bertsioa;
- SAP HANA Database, 1.0 eta 2.0 bertsioak;
- SAP NetWeaver Master Data Management Server, bertsioak: 710 eta 710.750.

Azalpena:

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

Konponbidea:

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

Alderantzizko *tabnabbing* motako ahultasunetarako, posible da honako arintze-neurriak aplikatzea:

- HTML:
  - *HTML loturetan rel atributua gehitzea: < a rel="external" href="https://ourpartner.com" target="_self" rel="noopener noreferrer" >texto< /a >.HTTP goiburuan zuzenean gehitzea: Referrer-Policy: noreferrer.*
  - *Gainera, nabigatzaileen hornitzaile nagusi bat "rel=noopener" delakoaren jokabide inplizitu bat garatzen hasi da, target="blank" erabiltzekotan*
- JavaScript bertsioetan, honako funtzioaren bidez:

```
function openPopup(url, name, options){
// Leiho gorakorra ireki eta irekiera eta erreferentzia politikaren jarraibidea ezartzea.
var newWin = window.open(null, name, 'noopener,noreferrer,' options);
// Irekiera lotura berrezartzea.
newWin.opener = null;
// Orain kargatu url zuzena.
newWin.location = url; }
```

Xehetasuna:

SAPek, segurtasun-partxeen hileroko komunikazioan, 7 segurtasun-ohar eta 6 eguneratze egin ditu. Horietako 3 larritasun kritikokoak dira, 2 handikoak eta 8 tartekoak.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Click bahiketaren motako ahultasun bat,
- *Cross-site Scripting* motako ahultasun bat,
- Zerbitzu ukapenaren inguruko ahultasun bat,
- Baimenaren konprobatze faltaren 3 ahultasun,
- Kodearen urrutiko exekuzioaren ahultasun bat,
- SQL *injection* motako ahultasun bat,
- Beste motaren bateko 6 ahultasun.

Segurtasun ohar nabarmenenak honakoen ingurukoak dira:

- Egiaztatutako erasotzaile batek, SAP *Commerce Cloud* sisteman *drool* arauak editatzeko pribilegioekin, kode maltzurra injektatu lezake horietan. Horrela izanik, kodearen urrutiko exekuzioa gerta liteke arauak exekutatzen direnean, eta azpiko hosta konprometitu liteke eta aplikazioaren konfidentzialtasun, integritate eta eskuragarritasunari eragin liezaioke. Ahultasun horretarako, CVE-2021-21477 identifikatzailea esleitu da.
- Alderantzizko *tabnabbing* motako akats baten ondorioz, gerta liteke nabigatzailearen beste pestaina batean irekitzen den dokumentu lotu batek jatorrizko orrialdea ordeztu edo birbideratzea, *phishing* orri bat jarriz, erabiltzailearen aldetik inolako interakziorik izan gabe.

Etiketak: Eguneratzea, SAP, Ahultasuna

Kodearen urrutiko exekuzioa Micro Focusen Operations Bridge Manager sisteman

Argitalpen data: 2021/02/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Micro Focus Operations Bridge Manager (OBM), bertsioak:

- 2020.10 (soilik lehenetsitako konfigurazioa aldatu bada);
- 2020.05;
- 2019.11;
- 2019.05;
- 2018.11;
- 2018.05;
- 10.6x;
- 10.1x;
- Bertsio zaharragoak.

Azalpena:

Larritasun kritikoko ahultasun baten berri eman da. Horren bidez, erasotzaile batek urrutiko konexioa exekuta lezake

Konponbidea:

Fabrikatzaileak web orrian emandako jarraibideei kasu egitea.

Xehetasuna:

AzalpenaAhultasun baten bidez, urrutiko erasotzaile batek kode arbitrarioa exekuta lezake OBM zerbitzari batean. Ahultasun horretarako, CVE-2021-22504 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Egiaztatze-sistema saihestea Palo Alto Networks enpresaren Prisma Cloud Compute sisteman

Argitalpen data: 2021/02/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Prisma Cloud Compute, SAML egiaztatzea erabiliz, honako bertsioak:

- 19.11 < = 2 eguneratzea;
- 20.04 < = 2 eguneratzea;
- 20.09 < = 2 eguneratzea;
- 20.12 < = 1 eguneratzea;

Azalpena:

Palo Alto Networks erakundeak jakinarazi du larritasun kritikoko ahultasun bat antzeman dela, eta, horren bidez, erasotzaile batek SAML egiaztatzea saihestu lezakeela (*Security Assertion Markup Language*).

Konponbidea:

Prisma Cloud Compute 20.12 bertsiora eguneratzea (1 eguneratzea) edota osteko batera.

Arintze-neurri moduan, SAML egiaztatzea desaktibatzea erabiltzen da.

Xehetasuna:

Prisma Cloud Compute kontsolan sinadura digitalaren egiaztatze okerra gertatuz gero, erasotzaile batek sinaduraren balioztatzea saihestu lezake SAML egiaztatzean, eta, horrela izanik, baimendutako edozein erabiltzaileren moduan hasi lezake saioa. Ahultasun horretarako, CVE-2021-3033 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun Xen sisteman

Argitalpen data: 2021/02/17

Garrantzia: Altua

Kaltetutako baliabideak:

- Linux 3.2 eta aurreko bertsio guztiak, PV (x86), edo Arm gisa exekutatzen. HVM (Hardware Virtual Machine) / PVH (Paravirtualization on Hardware) gisa exekutatzen diren bertsioak ez dira ahulak.
- Linux 2.6.39 eta goragoko bertsioak PV gisa. HVM / PVH gisa exekutatzen diren Linux bertsioak ez dira ahulak.
- 4.18 Linux bertsioak eta goragokoak.
- Xen 4.9 bertsioa eta goragokoak, Arm sistemetan.
- 3.11 Linux bertsioak eta goragokoak.

Azalpena:

Xen sistemako hainbat ahultasunen ondorioz, erasotzaile batek zerbitzu ukapena lortu lezake, edo pribilegioetan gora egitea edo informazioa zabaltzea.

Konponbidea:

Dagokion eguneratzea instalatzea:

- xsa361-linux-1.patch;
- xsa361-linux-2.patch;
- xsa361-linux-3.patch;
- xsa361-linux-4.patch;
- xsa361-linux-5.patch;
- xsa362-linux-1.patch;
- xsa362-linux-2.patch;
- xsa362-linux-3.patch;
- xsa363.patch;
- xsa364.patch;
- xsa365-linux.patch.

Xehetasunak:

- Fronted kontrolatzaile maltzur edo akastun baten bidez, dagokion backned kontrolatzailea blokeatu daiteke, zerbitzuaren ukapena eraginez. Ahultasun horietarako CVE-2021-26932 eta CVE-2021-26931 identifikatzaileak erreserbatu dira.
- Fronted kontrolatzaile maltzur edo akastun baten bidez, dagokion backned kontrolatzailea blokeatu daiteke, host osoan zerbitzuaren ukapena eraginez. Pribilegioetan gora egitea eta informazio-ihesa ere gerta litezke. Ahultasun horretarako, CVE-2021-26930 identifikatzailea esleitu da.
- Linuxen drm_xen_front kontrolatzaileen backend esleipen-sistemaren balioztatze-faltaren bidez, konfigurazio baliozko bat baimendu liteke, benetan horretarako diseinatuta ez egon arren. Funtzio horren erabilerak zein eragin izan dezakeen ez dakigu. Ahultasun horretarako, CVE-2021-26934 identifikatzailea esleitu da.
- Cache garbiketa desegokiaren bidez, asmo txarreko gonbidatu batek aurretik beste gonbidatu batenak ziren memoriaren datu sentikorrak irakur litzake. Ahultasun horretarako, CVE-2021-26933 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Birtualizazioa, Ahultasuna

Hainbat ahultasun VMware produktuetan

Argitalpen data: 2021/02/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- vCenter Server, 6.5, 6.7 eta 7.0 bertsioak;
- Cloud Foundation (vCenter Server), 3.x eta 4.x bertsioak;
- ESXi, 6.5, 6.7 eta 7.0 bertsioak;
- Cloud Foundation (ESXi), 3.x eta 4.x bertsioak.

Azalpena:

Mikhail Klyuchnikov, Positive Technologies erakundeko ikertzaileak, eta Lucas Leong, Trend Micro erakundeko ikertzaileak, larritasun kritikoko, handiko eta tarteko larritasuneko ahultasun bana antzeman dituzte, kodearen urrutiko exekuzio, montikuluaren gainezkatze (heap) eta SSRF (Server Side Request Forgery) motakoak, hurrenez hurren.

Konponbidea:

Honako bertsioetara eguneratzea, kaltetutako produktuaren arabera:

- vCenter Server, 6.5 U3n, 6.7 U3l eta 7.0 U1c bertsioak;
- Cloud Foundation (vCenter Server), 3.10.1.2 eta 4.2 bertsioak;
- ESXi, ESXi650-202102101-SG, ESXi670-202102401-SG eta ESXi70U1c-17325551 bertsioak;
- Cloud Foundation (ESXi), KB82705 eta 4.2 bertsioak.

Xehetasunak:

- 443 porturako sarbidea duen erasotzaile batek vROPs sistemarako VCenter Server plugin bateko ahultasuna baliatu lezake (VMware vRealize Operations) eta VCenter Server sistema ostatatzen duen azpiko sistema eragilean pribilegioen murrizketarik gabeko komandoak exekutatu. Ahultasun kritiko horretarako, CVE-2021-21972 identifikatzailea esleitu da.
- ESXi-ren sare segmentu berean kokatutako erasotzaile batek, 427 porturako sarbidea duenak, montikuluaren gainezkatze motako ahultasuna baliatu lezake (heap*) OpenSLP zerbitzuan, eta kodearen urrutiko exekuzioa gertatuko litzateke. CVE-2021-21974 identifikatzailea esleitu da ahultasun handi horretarako.*
- 443 porturako sarbidea duen erasotzaile batek SSRF ahultasun bat baliatu lezake, VCenter Server sistemaren plugin bateko URLen balioztatze desegokiaren ondorioz, eta plugin horretarako POST eskaera bat bidali. Horrek, informazioa zabaltzea eragin lezake. Ahultasun horretarako CVE-2021-21973 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Birtualizazioa, VMware, Ahultasuna.

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2021/02/25

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Honako Cisco produktuak, Cisco NX-OS Software sistemaren 9.3(5) edo 9.3(6) bertsioak exekutatzen ari badira.
  - Nexus 3000 Series Switches,
  - Nexus 9000 Series Switches,NX-OS modu independentean.
- Cisco Application Services Engine Software, 1.1 (3d) bertsioa eta aurrekoak.
- Cisco ACI Multi-Site Orchestrator (MSO) 3.0 software bertsio bat exekutatuz, soilik Cisco Application Services Engine sisteman zabaldu bazen.

Azalpena:

Cisco produktuetan 4 ahultasun identifikatu dira, denak larritasun kritikokoak, eta, horien bidez, urrutiko erasotzaile batek artxibo aleatorioak sortu, ezabatu edo aldatu litzake, informazio sentikorra eskuratzeko sarbidea lortu, edota kaltetutako gailuan baimena ekidin.

Konponbidea:

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

Xehetasuna:

- Erasotzaile batek ahultasun hori baliatu lezake TCP paketeak bidaliz, bereziki diseinatuak, TCP 9075 portuko tokiko interfaze batean konfiguratutako IP helbide batera. Arrakastaz baliatuz gero, erasotzaileak artxibo arbitrarioak sortu, ezabatu edota gainidatz litzake, gailuaren konfigurazioarekin erlazionatutako artxibo sentikorrak barne. Ahultasun horretarako, CVE-2021-1361 identifikatzailea esleitu da.
- Erasotzaile batek ahultasun hori baliatu lezake bereziki diseinatutako TCP eskaerak zerbitzari zehatz batera bidaliz. Hori ondo baliatuta, erasotzaileak sarbide pribilegiatua eduki lezake containerrak exekutatu edota host mailako operazioak deitzeko. Ahultasun horretarako, CVE-2021-1393 identifikatzailea esleitu da.
- Erasotzaile batek ahultasun hori baliatu lezake bereziki diseinatutako HTTP eskaerak kaltetutako APIra bidaliz. Hori ondo baliatuta, erasotzaileak gailuaren inguruko informazio espezifikoa eskuratu lezake, euskarri teknikoko artxiboak sortu bolumen isolatu batean, eta konfigurazio aldaketak egin. Ahultasun horretarako, CVE-2021-1396 identifikatzailea esleitu da.
- Erasotzaile batek ahultasun hori baliatu lezake, bereziki diseinatutako eskaera bat kaltetutako APIra bidaliz. Ondo erabilita, erasotzaileak token bat jaso lezake administrari mailako pribilegioekin, eta kaltetutako MSO eta Cisco APIC gailuetan API sisteman sar liteke. Ahultasun horretarako, CVE-2021-1388 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Cisco, Ahultasuna