2020ko otsailaren Bulletina

Ohartarazpenak - Teknikoak

Bufferraren gainezkatze erako ahultasuna sudo-n

Argitalpen data: 2020/02/03

Garrantzia: Altua

Kaltetutako baliabideak:

sudo-ren 1.7.1etik 1.8.25p1-era bitarteko bertsioak, *sudoers* fitxategian *pwfeedback* aukera gaituta badago.

Azalpena:

Joe Vennix-ek kritikotasun altuko ahultasun bat aurkitu du *sudo*-n. Hori baliatuz erasotzaile batek pilan oinarritutako bufferraren gainezkatzea (*stack*) eragin lezake.

Konponbidea:

1.8.31 bertsiora eguneratzea.

Xehetasuna:

sudo-k duen pilan oinarritutako bufferraren gainezkatze (*stack*) erako ahultasun bat baliatuz, pribilegiorik gabeko erabiltzaile batek pribilegioen eskalatzea egin lezake eta *root* baimenak eskuratu. Horrek informazioaren kontrol osoa emango lioke *sudoers* fitxategian *pwfeedback* aukera gaituta duten kaltetutako bertsioetan. Ahultasun horretarako CVE-2019-18634 identifikatzailea erabili da.

Etiketak: Eguneraketa, Linux, Ahultasuna

Hainbat ahultasun Squid-en

Argitalpen data: 2020/02/04

Garrantzia: Altua

Kaltetutako baliabideak:

Squid-en ondoko bertsioak:

- 2.x bertsiotik 2.7.STABLE9ra bitartekoak;
- 3.x bertsiotik 3.5.28ra bitartekoak;
- 4.x bertsiotik 4.9ra bitartekoak.

Azalpena:

Squid proxy zerbitzariaren hainbat bertsiotan hiru ahultasun aurkitu dira. Horiek baliatuz erasotzaile batek sarbidearen segurtasun kontrolak saihets litzake, zerbitzuaren ukapena eragin edo informazioa hedatu.

Konponbidea:

4.10 bertsiora eguneratzea.

Xehetasuna:

- Sarreraren baliozkotze oker baten ondorioz, Squid-ek bereziki diseinatutako HTTP eskariak modu okerrean interpreta ditzake, aurreko segurtasun iragazkiek debekatutako zerbitzariaren baliabideetara sarbidea lortzeko. Gainera, bufferraren administrazio okerraren ondorioz, urruneko bezero batek bufferraren gainezkatze egoera eragin lezake alderantzizko proxy modura funtzionatzen duen Squid batean. Ahultasun horretarako CVE-2020-8449 eta CVE-2020-8450 identifikatzaileak erreserbatu dira.
- Datuen kudeaketa oker baten ondorioz, Squid ahula da informazio hedapenaren aurrean FTP zerbitzariaren zerrendak HTTP erantzunetara itzultzen dituenean. Ahultasun horretarako CVE-2019-12528 identifikatzailea erreserbatu da.

- Bufferraren kudeaketa okerraren ondorioz, *ext_lm_group_acl* fitxategi bitarra ahula da zerbitzuaren ukapen erako eraso baten aurrean, NTLM (*NT LAN Manager*) autentifikazio kredentzialak prozesatzen direnean. Ahultasun horretarako CVE-2020-8517 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun Cisco-ren produktuetan

Argitalpen data: 2020/02/06

Garrantzia: Altua

Kaltetutako baliabideak:

- ASR 9000 Series Aggregation Services Routers;
- Carrier Routing System (CRS);
- Firepower 4100 Series;
- Firepower 9300 Security Appliances;
- IOS XRv 9000 Router;
- MDS 9000 Series Multilayer Switches;
- Network Convergence System (NCS) Series Routers:
  - 540 Series Routers;
  - 560 Series Routers;
  - 1000 Series;
  - 5000 Series;
  - 5500 Series;
  - 6000 Series;
- Nexus 1000 Virtual Edge para VMware vSphere;
- Nexus 1000V Switch para Microsoft Hyper-V;
- Nexus 1000V Switch para VMware vSphere;
- Nexus 3000 Series Switches;
- Nexus 5500 Plataform Switches;
- Nexus 5600 Plataform Switches;
- Nexus 6000 Series Switches;
- Nexus 7000 Series Switches;
- Nexus 9000 Series Fabric Switches Application Centric Infrastructure (ACI) moduan;
- Nexus 9000 Series Switches independiente NX-OS moduan:
- UCS 6200 Series Fabric Interconnects;
- UCS 6300 Series Fabric Interconnects;
- UCS 6400 Series Fabric Interconnects;
- Network Convergence System (NCS) Series Routers:
  - 1000;
  - 5000;
  - 5500;
  - 6000;
- Video Surveillance 3000 Series IP Cameras;
- Video Surveillance 4000 Series High-Definition IP Cameras;
- Video Surveillance 4300E and 4500E High-Definition IP Cameras;
- Video Surveillance 6000 Series IP Cameras;
- Video Surveillance 7000 Series IP Cameras;
- Video Surveillance PTZ IP Cameras;
- IP Conference Phone 7832;
- IP Conference Phone 7832 anitzeko firmwarearekin
- IP Conference Phone 8832;
- IP Conference Phone 8832 plataforma anitzeko firmwarearekin;;
- IP Phone 6821, 6841, 6851, 6861, 6871 plataforma anitzeko firmwarearekin;
- IP Phone 7811, 7821, 7841, 7861 Desktop Phones;
- IP Phone 7811, 7821, 7841, 7861 Desktop Phones plataforma anitzeko firmwarearekin;
- IP Phone 8811, 8841, 8851, 8861, 8845, 8865 Desktop Phones;
- IP Phone 8811, 8841, 8851, 8861, 8845, 8865 Desktop Phones plataforma anitzeko firmwarearekin;
- Unified IP Conference Phone 8831;
- Unified IP Conference Phone 8831 hirugarrenen deien kontrolerako;
- Wireless IP Phone 8821, 8821-EX.

Azalpena:

Armis-eko bi ikertzailek, Barak Hadad eta Ben Seri, Cisco-ri kritikotasun altuko bost ahultasunen berri eman diote. Autentifikatu gabeko gertuko erasotzaile batek zerbitzuaren ukapen egoera sor lezake, kode arbitrarioa exekutatu, baita *root* pribilegioekin ere, eta gailuetan berrabiatzeak eragin.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Software de Cisco-ren deskarga paneletik deskarga daitezke.

Xehetasuna:

- Cisco Discovery Protocol-en mezuen prozesamenduan egiaztapen falta bat baliatuz, autentifikatu gabeko gertuko erasotzaile batek asmo gaiztoko paketeak bidal litzake eta berrabiatzeak eragin, edo zerbitzuaren ukapen egoera (DoS) eragin gailuan. Ahultasun horretarako CVE-2020-3120 identifikatzailea erabili da.
- Cisco Discovery Protocol-en mezuen eremu batzuetan dagoen sarrera kateen baliozkotze oker bat baliatuz, autentifikatu gabeko gertuko erasotzaile batek asmo gaiztoko paketeak bidal litzake eta kodearen exekuzio arbitrarioa egin lezake gailuan administratzaile pribilegioekin. Ahultasun horretarako CVE-2020-3118 kodea erabili da.
- Cisco Discovery Protocol-en mezuen prozesamenduan egiaztapen falta bat baliatuz, autentifikatu gabeko gertuko erasotzaile batek asmo gaiztoko paketeak bidal litzake eta berrabiatzeak eragin, edo zerbitzuaren ukapen egoera (DoS) eragin gailuan. Ahultasun horretarako CVE-2020-3110 identifikatzailea erabili da.
- Cisco Discovery Protocol-en mezuen sarrera batzuetako eremuen baliozkotze oker bat baliatuz, autentifikatu gabeko gertuko erasotzaile batek asmo gaiztoko paketeak bidal litzake eta kodearen exekuzio arbitrarioa egin lezake gailuan administratzaile pribilegioekin. Ahultasun horretarako CVE-2020-3119 identifikatzailea erabili da.
- Cisco Discovery Protocol-en mezuen prozesamenduan egiaztapen falta bat baliatuz, autentifikatu gabeko gertuko erasotzaile batek asmo gaiztoko paketeak bidal litzake eta berrabiatzeak eragin, zerbitzuaren ukapen egoera (DoS) eragin, edo kodearen exekuzio

arbitrarioa egin lezake gailuan *root* pribilegioekin. Ahultasun horretarako CVE-2020-3111 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Ahultasuna Aruba-ren switchetan

Argitalpen data: 2020/02/12

Garrantzia: Altua

Kaltetutako baliabideak:

Aruba Intelligent Edge Switches:

- 5400R,
- 3810,
- 2920,
- 2930,
- 2530 GigT Por-ekin,
- 2530 10/100 port,
- 2540.

Firmwarearen ondorengo bertsioetarako:.

- 16.08.*, 16.08.0009 baino lehenagokoak;
- 16.09.*, 16.09.0007 baino lehenagokoak;
- 16.10.*, 16.10.0003 baino lehenagokoak.

Azalpena:

Aruba produktuek duten ahultasun baten berri eman da. Hori baliatuz urruneko erasotzaile batek informazioa heda lezake.

Konponbidea:

Firmwarearen honako bertsio hauetara eguneratzea:

- 16.08.0009,
- 16.09.0007,
- 16.10.0003.

Xehetasuna:

Kaltetutako switchen webaren kudeaketa interfazeak duen informazioaren hedapen erako ahultasun bat baliatuz, urruneko erasotzaile batek sistemaren informazioa berreskura lezake, interfaze horretara bereziki prestatutako pakete bat bidaliz. Baldintza oso berezietan ahultasuna baliatua izan liteke autentifikazioaren beharrik gabe. Ahultasun horretarako CVE-2019-5322 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Microsoften 2020ko otsaileko segurtasun buletina

Argitalpen data: 2020/02/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows;
- Microsoft Edge (EdgeHTMLn oinarritua);
- Microsoft Edge(Chromium-en oinarritua);
- ChakraCore;
- Internet Explorer;
- Microsoft Exchange Server;
- Microsoft SQL Server;
- Microsoft Office, Microsoft Office Services eta Web Apps;
- Windows Malicious Software Removal Tool;
- Windows Surface Hub.

Azalpena:

Segurtasun eguneraketei buruzko Microsoften otsaileko argitalpenean 101 ahultasun jaso dira, 13 kritiko gisa sailkatu dira eta 88 garrantzitsu gisa.

Solución:

Dagozkien segurtasun eguneraketak instalatzea. Microsoft-en orrialdean eguneraketa horiek egiteko metodo ezberdinei buruzko argibideak daude.

Xehetasuna:

Argitaratutako ahultasun motak honako hauek dira:

- kodearen urruneko exekuzioa,
- pribilegioen eskalatzea,
- zerbitzuaren ukapena,
- informazioaren zabalkundea,
- segurtasun ezaugarria saihestea,
- identitatea ordeztea *(spoofing),*
- informazioa manipulatzea *(tampering)*.

Etiketak: Eguneraketa, Microsoft, Nabigatzailea, Ahultasuna, Windows

Ahultasuna Intel-en CSME azpisistemetan

Argitalpen data: 2020/02/12

Garrantzia: Altua

Kaltetutako baliabideak:

- Intel CSME, honakoak baino lehenagoko bertsioak:
  - 12.0.49;
  - 12.0.56, IOTrako soilik;
  - 13.0.21;
  - 14.0.11.

Azalpena:

Chedva Gottesman ikertzaileak, Intel-ekin lankidetzan, kritikotasun altuko ahultasun bat aurkitu du CSME azpisistemetan. Hori baliatuz erasotzaile lokal batek pribilegioen eskalatzea egin lezake, zerbitzuaren ukapen egoera eragin edo informazioa zabaldu.

Konponbidea:

CSME honako bertsioetara eguneratzea:

- 2.0.49,
- 13.0.21,
- 14.0.11.

edo ondorengoak.

- CSME IOTren kasuan, 12.0.56 edo bertsio berriagoetara eguneratzea.

Xehetasuna:

Autentifikazio oker bat baliatuz erasotzaile lokal batek pribilegioen eskalatzea egin lezake, zerbitzuaren ukapena eragin edo informazioa hedatu. Ahultasun horretarako CVE-2019-14598 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

SAPen 2020ko otsaileko segurtasun eguneraketa

Argitalpen data: 2020/02/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Business Client, 6.5 bertsioa;
- SAP Host Agent, 7.21 bertsioa;
- SAP Landscape Management, 3.0 bertsioa;
- ABAP Server (NetWeaver eta Suite/ERP-n erabilia), honako bertsioak;
  - Kernel 7.21 edo 7.22 erabiliz, ABAP Server erabiltzen duena 7.00 bertsiotik 7.31 bertsiora bitartean;
  - Kernel 7.45, 7.49 edo 7.53 erabiliz, ABAP Server erabiltzen duena 7.40 bertsiotik 7.52 bertsiora bitartean;
  - ABAP Platform.
- SAP ERP, SAP_APPL 600, 602, 603, 604, 605, 606, 616, SAP_FIN 617, 618, 700, 720 eta 730 bertsioak;
- SAP S/4 HANA, honako bertsioak:
  - S4CORE 100, 101, 102, 103, 104;
  - SAP_BASIS 7.50, 7.51, 7.52, 7.53, 7.54.
- SAP NetWeaver, honako bertsioak:
  - 7.30, 7.31, 7.40 eta 7.50 (Knowledge Management ICE Service);
  - SAP_BASIS 7.40;
  - SAP_BASIS 702, 730, 731 eta 740;
  - 7.30, 7.31, 7.40 eta 7.50 (Heap Dump Application);
  - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50 (Guided Procedures).
- SAP Business Objects Business Intelligence Platform (CMC), 4.2 bertsioa;
- SAP Mobile Platform, 3.0 bertsioa.

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 13 segurtasun ohar eta 2 eguneraketa eman ditu ezagutzera. Eguneraketetako bat larritasun kritikokoa da, 3 ohar larritasun altukoak dira, eta beste eguneraketa eta gainerako oharrak larritasun ertainekoak dira.

Argitaratutako ahultasun motak honako hauek dira:

- *DoS (Denial of Service)* erako 3 ahultasun;
- sarrera datuen egiaztapen gabeziako 2 ahultasun;
- *XSS (Cross-Site Scripting)* erako 2 ahultasun;
- autentifikazioaren egiaztapen gabeziako ahultasun bat;

- HTTP erantzunaren zatiketa erako ahultasun bat;
- beste era batzuetako 6 ahultasun.

Ahultasun horietarako honako identifikatzaileak erreserbatu dira: CVE-2020-6186, CVE-2020-6191, CVE-2020-6192, CVE-2020-6188, CVE-2020-6193, CVE-2020-6184, CVE-2020-6185, CVE-2020-6181, CVE-2020-6190, CVE-2020-6183, CVE-2020-6189, CVE-2020-6187 eta CVE-2020-6177.CVE-2019-0271 identifikatzailea esleitua izan da.

Etiketak: Eguneraketa, SAP, Ahultasuna

Autentifikazioaren gabezia erako ahultasuna IBM Tivoli Monitoring Service-n

Argitalpen data: 2020/02/13

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Tivoli Monitoring Service, honako bertsioak:

- 6.3.0 Fix Pack 7, Service Packs 1 eta 2;
- 6.3.0.7-TIV-ITM_TEMA-IF0003 bertsiotik 6.3.0.7-TIV-ITM_TEMA-IF0009 bertsiora bitartekoak.

Azalpena:

Ehsan Razaghik larritasun altuko ahultasun baten berri eman du, IBMren Tivoli Monitoring Service produktuari eragiten diona.

Konponbidea:

IBM Tivoli Monitoring Service 6.3.0 Fix Pack 7 Service Pack 3 (6.3.0.7-TIV-ITM-SP0003) bertsiora eguneratzea.

Xehetasuna:

IBM Tivoli Monitoring Servicek duen autentifikazioaren gabezia erako ahultasun bat baliatuz, erasotzaile bat ITMren monitorizazio zerbitzariaren alderdi operatiboetara sar liteke eta horiek aldatu. Horrek zerbitzuaren ukapen egoera eragingo luke edo monitorizazio zerbitzaria desaktibatzea. Ahultasun horretarako CVE-2019-4592 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

CSRFren aurreko babes ez-nahikoa Palo Alto-ren Expedition Migration Tool-en

Argitalpen data: 2020/02/13

Garrantzia: Altua

Kaltetutako baliabideak:

Expedition Migration Tool, 1.1.51 eta lehenagoko bertsioak.

Azalpena:

Tenable-ko Jimi Sebree ikertzaileak kritikotasun altuko ahultasun bat aurkitu du. Autentifikatu gabeko urruneko erasotzaile batek administratzaileen autentifikazioa bahitu lezake eta tresnan ekintzan egin.

Konponbidea:

Expedition Migration Tool 1.1.52 edo geroagoko bertsiora eguneratzea.

Xehetasuna:

Cross-Site Request Forgery-ren (CSRF) aurreko babes ez-nahiko bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek administratzaileen autentifikazioa bahitu lezake eta tresnan ekintzak egin.

Etiketak: Eguneraketa, Ahultasuna

SQL injekzio erako ahultasuna IBMren hainbat produktutan

Argitalpen data: 2020/02/20

Garrantzia: Altua

Kaltetutako baliabideak:

- IBM Emptoris Spend Analysis, honako bertsioak:
  - 10.1.0.x;
  - 10.1.1.x;
  - 10.1.3.x.

- IBM Emptoris Strategic Supply Management Platform, honako bertsioak:
  - 10.1.0.x;
  - 10.1.1.x;
  - 10.1.3.x.

Azalpena:

IBM Emptoris Spend Analysis eta IBM Emptoris Strategic Supply Management Platform produktuek larritasun altuko ahultasun bat daukate, SQL injekzio erakoa.

Konponbidea:

- IBM Emptoris Spend Analysis, honako bertsioetara eguneratzea:
  - 10.1.0.34;
  - 10.1.1.33;
  - 10.1.3.29.
- IBM Emptoris Strategic Supply Management Platform, honako bertsioetara eguneratzea:
  - 10.1.0.34;
  - 10.1.1.33;
  - 10.1.3.29.

Xehetasuna:

Urruneko erasotzaile batek bereziki prestatutako SQL eskaerak bidal litzake, eta horrela *backend*-eko datu basean informazioa ikusi, gehitu, aldatu edo ezabatu lezake. Ahultasun horretarako CVE-2019-4752 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2020/02/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco Smart Software Manager On-Prem, 7-202001 baino lehenagoko bertsioak High Availability (HA) aukera aktibatuta badute;
- Cisco Unified Contact Center Express Software, 12.5(1) baino lehenagoko bertsioak;
- Firepower Management Center (FMC) 1000;
- Firepower Management Center (FMC) 2500;
- Firepower Management Center (FMC) 4500;
- Secure Network Server 3500 Series Appliances;
- Secure Network Server 3600 Series Appliances;
- Threat Grid 5504 Appliance;
- Cisco ESA eta Cisco SMA, gailu birtualak eta hardwarekoak, Cisco AMP erabiltzeko edo mezuen segimendurako konfiguratutako Cisco AsyncOS softwarearen bertsio ahul bat exekutatzen ari direnean.
- Cisco AsyncOS Software, Cisco Email Security Appliance-rako (ESA) 12.1.0-085 eta 11.1.0-131 bertsioak;
- Cisco DCNM software, Release 11.3(1) baino lehenagoko bertsioak.

Azalpena:

Hainbat ahultasun aurkitu dira Cisco produktuetan, horietatik 1 larritasun kritikokoa eta 6 larritasun altukoak.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Software Cisco-ren deskargen paneletik deskarga daitezke.

Xehetasuna:

- Lehenetsitako pasahitz estatikoa duen sistemaren kontu bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek sistemaren informazio sentikorrera sarbidea lor lezake pribilegio altuak dituen kontu batekin. Ahultasun horretarako CVE-2020-3158 identifikatzailea erabili da.
- Edukiak igotzerakoan murrizpen nahikoak ez daudela baliatuz, autentifikatu gabeko urruneko erasotzaile batek fitxategi arbitrarioak karga litzake eta komandoak exekutatu azpiko sistema eragilean. Ahultasun horretarako CVE-2019-1888 identifikatzailea erabili da.
- Firmwarea eguneratzeko zerbitzariaren irudien baliozkotze ez-aski bat baliatuz, autentifikatu gabeko erasotzaile fisiko batek abiatze seguruko Unified Extensible Firmware Interface (UEFI) egiaztapenak saihets litzake, eta softwarearen irudi arriskutsu bat kargatu kaltetutako gailu batean. Ahultasun horretarako CVE-2019-1736 identifikatzailea erabili da.
- Mezu elektronikoen atxikien baliozkotze ez-aski bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek bereziki diseinatutako atxikiak bidal litzake ustekabeko itxierak eragiteko produktuaren barne prozesuetan, eta horrela zerbitzuaren ukapena eragin. Ahultasun horretarako CVE-2019-1983 identifikatzailea erabili da.
- Tamaina handiko atxikiak dituzten mezu elektronikoen baliozkotze desegoki bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek CPUaren erabilpena %100eraino handitu lezake, eta horrela zerbitzuaren ukapena eragin. Ahultasun horretarako CVE-2019-1947 identifikatzailea erabili da.
- Sarbidearen kontrolean baliozkotze ez-aski bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek pribilegioak eskala litzake aplikazioan, REST APIra bereziki diseinatutako eskaerak bidaliz. Ahultasun horretarako CVE-2020-3112 identifikatzailea erabili da.
- Web interfazearen CSRF babes ez-aski bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek cross-site request forgery erako erasoak egin litzake sisteman eta ekintza arbitrarioak egitea lor lezake kaltetutako erabiltzailearen baimen berdinekin. Ahultasun horretarako CVE-2020-3114 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun VMware-ren Horizon Adapter-erako vRealize Operations-en

Argitalpen data: 2020/02/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Horizon Adapter-erako vRealize Operations, honako bertsioak:

- 6.6.x;
- 6.7.x.

Azalpena:

Larritasun kritiko, altu eta ertaineko 3 ahultasun aurkitu dira, kodearen urruneko exekuzio, autentifikazioaren saihespen eta informazioaren hedapen erakoak, hurrenez hurren.

Konponbidea:

Kaltetutako produktua ondoko bertsioetara eguneratzea:

- 6.6.1;
- 6.7.1.

Xehetasuna:

- vRealize Operations-en sarera sarbidea lukeen autentifikatu gabeko urruneko erasotzaile batek, Horizon Adapter funtzionatzen ari bada, kode arbitrarioa exekuta lezake vRealize Operations-en. Ahultasun horretarako CVE-2020-3943 identifikatzailea erabili da.
- vRealize Operations-en sarera sarbidea lukeen autentifikatu gabeko urruneko erasotzaile batek, Horizon Adapterrekin funtzionatzen ari bada, Horizon Adapter-en autentifikazioa saihets lezake, entitate ziurtatzaileen konfiantza errepositorioaren (trust store) konfigurazio desegoki bat baliatuz. Ahultasun horretarako CVE-2020-3944 identifikatzailea erabili da.

Larritasun ertaineko ahultasunerako CVE-2020-3945 identifikatzailea erabili da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Cross-Site Scripting erako ahultasuna TIBCO EBX-en

Argitalpen data: 2020/02/20

Garrantzia: Altua

Kaltetutako baliabideak:

- TIBCO EBX, honako bertsioak:
  - 5.8.1.fixS eta lehenagokoak;
  - 5.9.3, 5.9.4, 5.9.5, 5.9.6 eta 5.9.7.
- Web server osagaia.

Azalpena:

Larritasun altuko ahultasun bat argitaratu da, eta hori baliatuz autentifikatu gabeko erasotzaile batek gordetako cross-site scripting erako erasoak egin litzake.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- TIBCO EBX, 5.8.1.fixT edo ondorengo bertsioak;
- TIBCO EBX, 5.9.8 edo ondorengo bertsioak.

Xehetasuna:

Kaltetutako produktuek duten ahultasun bat baliatuz, autentifikatu gabeko erasotzaile batek gordetako cross-site scripting erasoak egin litzake. Ahultasun horretarako CVE-2019-17333 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Komandoen injekzio erako ahultasuna IBM Spectrum Protect Plus-en

Argitalpen data: 2020/02/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

IBM Spectrum Protect Plus, 10.1.0 bertsiotik 10.1.5 bertsiora bitartekoak.

Azalpena:

Hainbat ahultasunek, guztiak larritasun kritikokoak eta komandoen injekzio erakoak, urruneko erasotzaile bati ahalbidetu diezaiokete kode arbitrarioa exekutatzea kaltetutako sisteman.

Konponbidea:

IBM Spectrum Protect Plus 10.1.5 *patch1* bertsiora eguneratzea.

Xehetasuna:

IBM Spectrum Protect Plus-ek dituen komandoen injekzio erako hainbat ahultasun baliatuz, urruneko erasotzaile batek kode arbitrarioa exekuta lezake sisteman, bereziki diseinatutako HTTP komando bat erabiliz. Ahultasun horietarako CVE-2020-4210, CVE-2020-4213, CVE-2020-4222, CVE-2020-4212 eta CVE-2020-4211 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, IBM, Ahultasuna

Ahultasuna Dell-en Isilon OneFS-ren SyncIQ-n

Argitalpen data: 2020/02/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Dell EMC Isilon OneFS, 8.2.2 bertsiora bitarteko guztiak.

Azalpena:

Dell-ek larritasun kritikoko ahultasun bat aurkitu du SyncIQ-n, eta hori baliatuz urruneko erasotzaile batek sistemara baimenik gabeko sarbidea lor lezake.

Konponbidea:

Dell-ek hainbat eguneraketa eta gomendio argitaratu ditu, produktuaren bertsio eta ezaugarrien arabera. Informazio gehiago eskuratzeko *Erreferentziak* atala irakurri.

Xehetasuna:

Ahultasunak eragiten die SyncIQ duten OneFSren bertsioei. Urruneko erasotzaile batek baimenik gabeko sarbidea lor lezake eta ekintzak egin litzake sisteman. Ahultasun horretarako CVE-2020-5328 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Kodearen urruneko exekuzioa Apache Tomcat-en AJP-n

Argitalpen data: 2020/02/25

Garrantzia: Altua

Kaltetutako baliabideak:

Apache Tomcat, honako bertsioak:

- 7.0.0 bertsiotik 7.0.99 bertsiora bitartekoak,
- 8.5.0 bertsiotik 8.5.50 bertsiora bitartekoak,
- 9.0.0.M1 bertsiotik 9.0.30 bertsiora bitartekoak.

Azalpena:

Apache Tomcat-en segurtasun ekipoak larritasun altuko ahultasun bat aurkitu du Apache JServ Protocol-en (AJP). Hori baliatuz erasotzaile batek kodearen urruneko exekuzioa egin lezake.

Konponbidea:

Honako bertsio hauetara eguneratzea:

- 7.0.100,
- 8.5.51,
- 9.0.31.

Xehetasuna:

Apache Tomcat-ek AJP konexioak tratatzen ditu antzeko HTTP konexio batek, adibidez, baino konfiantza maila handiagoa balute bezala. Erasotzaile batek konexio horietara sarbidea balu, kodearen urruneko exekuzioa egin lezake eta horrela web aplikazioaren edozein parteko fitxategi arbitrarioetara sarbidea lortuko luke. Ahultasun horretarako CVE-2020-1938 identifikatzailea erabili da.

Etiketak: Eguneraketa, Apache, Ahultasuna

Hainbat ahultasun OpenSMTPD-n

Argitalpen data: 2020/02/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

OpenBSD 6.6.

Azalpena:

OpenBSD-k dituen larritasun kritiko eta baxuko hainbat ahultasun argitaratu dira. Horiek baliatuz, urruneko erasotzaile batek kaltetutako [illegible] io lokala ezagutzera eman.

Konponbidea:

[illegible] ile lokal batek fitxategi arbitrario bat [illegible] akur (adibidez, root-en pasahitzaren hash-a */etc/master.passwd-en*), edo beste erabiltzaile baten fitxateg [illegible] ategi

- Larritasun kritikoko ahultasuna *smtpd*-en mugez kanpoko irakurketa bat da. Hori baliatuz urruneko erasotzaile batek komando arbitrarioak injekta litzake fitxategietan, ondoren root modura exekutatzen direnak. Bestalde, smtpctl-en pribilegioak ez baliogabetzeak ahalbidetzen du komandoak exekutatzea *_smtpctl* taldearekin. Ahultasun horretarako CVE-2020-8794 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2020/02/27

Garrantzia: Altua

Kaltetutako baliabideak:

- Firepower
  - 1000 Series;
  - 2100 Series;
  - 4100 Series;
  - 9300 Security Appliances.
- Nexus
  - VMware vSphere-rako 1000 Virtual Edge;
  - Microsoft Hyper-V-rako 1000V Switch;
  - VMware vSphere-rako 1000V Switch;
  - 3000 Series Switches;
  - 5500 Platform Switches;
  - 5600 Platform Switches;
  - 6000 Series Switches;
  - 7000 Series Switches;
  - 9000 Series Fabric Switches, Application Centric Infrastructure (ACI) moduan;
  - 9000 Series Switches, NX-OS independente moduan.
- UCS
  - 6200 Series Fabric Interconnects;
  - 6300 Series Fabric Interconnects;
  - 6400 Series Fabric Interconnects.
- MDS 9000 Series Multilayer Switches.

Azalpena:

Cisco produktuetan 6 ahultasun aurkitu dira, denak larritasun altukoak, kodearen exekuzio arbitrario, zerbitzuaren ukapen eta komandoen injekzio erakoak.

Konponbidea:

Aipatutako ahultasunak konpontzen dituzten eguneraketak Software Cisco-ren deskargen paneletik deskarga daitezke.

Xehetasuna:

- Autentifikatu gabeko alboko erasotzaile batek kode arbitrarioa exekuta lezake root modura edo zerbitzuaren ukapen egoera (DoS) eragin lezake, kaltetutako produktuen paketeen goiburuetako baliozkotze ez-aski baten ondorioz. Ahultasun horretarako CVE-2020-3172 identifikatzailea erabili da.
- Sarreraren baliozkotze ez-aski baten ondorioz gertatzen den CLIren (Command Line Interface) kudeaketa lokaleko ahultasun bat baliatuz, autentifikatu gabeko erasotzaile lokal batek komando arbitrarioak exekuta litzake. Ahultasun horretarako CVE-2020-3171 identifikatzailea erabili da.
- Autentifikatu gabeko erasotzaile lokal batek CLI-n dagoen ahultasuna balia lezake eta komando arbitrarioak exekutatu kaltetutako produktuan. Ahultasun horretarako CVE-2020-3167 identifikatzailea erabili da.
- Baliabideen erabilpenaren kontrol desegoki bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake kaltetutako sisteman. Ahultasun horretarako CVE-2020-3175 identifikatzailea erabili da.
- Autentifikatu gabeko urruneko erasotzaile batek zerbitzuaren ukapen egoera (DoS) eragin lezake baliabideen esleipen oker baten ondorioz, CLIren saio hasieran akastun saioak dauden bitartean. Ahultasun horretarako CVE-2020-3168 identifikatzailea erabili da.
- Komandoen argumentuetan baliozkotze ez-aski bat baliatuz, autentifikatutako erasotzaile lokal batek komando arbitrarioak exekuta litzake kaltetutako gailuan. Ahultasun horretarako CVE-2020-3173 identifikatzailea erabili da.

Etiketak: Eguneraketa, Cisco, Ahultasuna