2020ko Apirilaren Bulletina

Ohartarazpenak - Teknikoak

DTLS protokoloaren segurtasun falta erako ahultasuna GnuTLS-n

Argitalpen data: 2020/04/01

Garrantzia: Altua

Kaltetutako baliabideak:

GnuTLS, 3.6.3 bertsioa.

Azalpena:

Larritasun altuko ahultasun bat aurkitu da GnuTLS-k erabiltzen duen DTLS protokoloan.

Konponbidea:

GnuTLS 3.6.13 edo geroagoko bertsioetara eguneratzea.

Xehetasuna:

GnuTLS 3.6.3-k DTLS (*Datagram Transport Layer Security*) protokoloaren inplementazioan erregresio bat sartu zuela antzeman dute. Horren ondorioz DTLS bezeroak ez du laguntzen DTLS negoziazioan, DTLS protokoloaren segurtasun bermeak hautsiz.

Etiketak: Eguneraketa, SSL/TLS, Ahultasuna

Bufferraren gainezkatzea IBMren hainbat Aspera aplikaziotan

Argitalpen data: 2020/04/01

Garrantzia: Altua

Kaltetutako baliabideak:

Ondoko produktuen bertsio guztiak:

- Aspera High Speed Transfer Server,
- Aspera High Speed Transfer Endpoint,
- Aspera Proxy,
- Aspera Transfer Cluster Manager,
- Aspera Application on Demand,
- Aspera Faspex on Demand,
- Aspera Server on Demand,
- Aspera Shares on Demand,
- Aspera Streaming,
- Cloudpak for Integration-erako (CP4I) Aspera High Speed Transfer Server.

Azalpena:

IBMk kritikotasun altuko ahultasun bat aurkitu du, bere Aspera aplikazio batzuei eragiten diena. Aspera-ri buruzko ezagupenak lituzkeen urruneko erasotzaile batek komandoak exekuta litzake *apshell shell* murriztu batean.

Konponbidea:

IBMk partxe sorta bat argitaratu du ahultasuna konpontzeko, kaltetutako produktuaren arabera. Partxe horiek eskuratzeko IBMk eskaini duen laguntza orrian eskura daitezke.

Xehetasuna:

Aspera aplikazio batzuk ahulak dira bufferraren gainezkatze baten aurrean. Aspera-ri buruzko ezagupenak lituzkeen urruneko erasotzaile batek komandoak exekuta litzake apshell shell murriztu batean. Ahultasun horretarako CVE-2020-4356 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Urruneko sarbidearen murrizpenaren saihespena HPE produktuetan

Argitalpen data: 2020/04/01

Garrantzia: Altua

Kaltetutako baliabideak:

- HPE MSA 1040 SAN Storage GL225P001 eta lehenagokoak,
- HPE MSA 2040 SAN Storage GL225P001 eta lehenagokoak,
- HPE MSA 2042 SAN Storage GL225P001 eta lehenagokoak,
- HPE MSA 1050 SAN Storage VE270R001-01 eta lehenagokoak,
- HPE MSA 2050 SAN Storage VL270R001-01 eta lehenagokoak,
- HPE MSA 2052 SAN Storage VL270R001-01 eta lehenagokoak.

Azalpena:

HPEk ezagutzera eman ditu kaltetutako produktuek dituzten urruneko sarbidearen murrizpenaren saihespen erako hainbat ahultasun.

Konponbidea:

- HPE MSA 1040, firmwarearen GL225P002-02 edo geroagoko bertsioa;
- HPE MSA 2040, firmwarearen GL225P002-02 edo geroagoko bertsioa;
- HPE MSA 2042, firmwarearen GL225P002-02 edo geroagoko bertsioa;
- HPE MSA 1050, firmwarearen VE270P002-02 edo geroagoko bertsioa;
- HPE MSA 2050, firmwarearen VL270P002-02 edo geroagoko bertsioa;
- HPE MSA 2052, firmwarearen VL270P002-02 edo geroagoko bertsioa.

Xehetasuna:

Kaltetutako produktuetan saioaren logikaren segurtasun erako eta urruneko saioaren tokenen berrerabilpen erako ahultasun posible batzuk aurkitu dira. Ahultasun horietarako CVE-2019-12001 eta CVE-2019-12002 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, HP, Ahultasuna

Ahultasuna DrayTek gailuetan

Argitalpen data: 2020/04/02

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Vigor3900, firmwarearen 1.5.1 bertsioa baino lehenagokoa dutenak;
- Vigor2960, firmwarearen 1.5.1 bertsioa baino lehenagokoa dutenak;
- Vigor300B, firmwarearen 1.5.1 bertsioa baino lehenagokoa dutenak.

Azalpena:

DrayTek-ek larritasun kritikoko ahultasun bat aurkitu du routerren Vigor familiako modelo batzuei eragiten diena. Urruneko erasotzaile batek sistemaren kontrola eskura lezake.

Solución:

- Vigor3900, firmwarearen 1.5.1 edo goragoko bertsiora eguneratzea;
- Vigor2960, firmwarearen 1.5.1 edo goragoko bertsiora eguneratzea;
- Vigor300B, firmwarearen 1.5.1 edo goragoko bertsiora eguneratzea.

Xehetasuna:

Gailuaren web erabiltzailearen interfazeak (WebUI) duen ahultasun bat baliatuz, urruneko erasotzaile batek sistemaren kontrola har lezake. Ahultasun horretarako CVE-2020-8515 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Komandoen exekuzioa root modura IBM Spectrum Scale-n

Argitalpen data: 2020/04/03

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Spectrum Scale, bertsio guztiak.

Azalpena:

Larritasun altuko ahultasun bat identifikatu da IBM Sprectum Scale-ren bertsio guztietan. Hori baliatuz pribilegiorik gabeko erasotzaile batek komandoak exekuta litzake *root* modura.

Konponbidea:

- 5.0.0.0tik 5.0.4.2ra bitarteko bertsioen kasuan, 5.0.4.3 bertsiora eguneratzea;
- 4.2.0.0tik 4.2.3.20ra bitarteko bertsioen kasuan, 4.2.3.21 bertsiora eguneratzea.

Xehetasuna:

IBM Sprectum Scale-k pribilegiorik gabeko erasotzaile lokal bati ahalbidetuko lioke, ingurunearen ezagutza handia izango balu, komandoak exekutazea root modura, bereziki diseinatutako sarrera datuak erabiliz. Ahultasun horretarako CVE-2020-4273 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Irakurketa eta idazketa gainezkatzea SolarWinds Dameware-n

Argitalpen data: 2020/04/07

Garrantzia: Altua

Kaltetutako baliabideak:

SolarWinds Dameware, 12.1 Hotfix 3 bertsioa.

Azalpena:

SolarWinds Dameware-k larritasun altuko ahultasun bat dauka, bufferrean irakurketaren eta idazketaren gainezkatze erakoa. Horrek zerbitzuaren ukapen egoera (DoS) eragin lezake.

Konponbidea:

Kaltetutako produktua 12.1.1 bertsiora eguneratzea.

Xehetasuna:

DWRCS.exe-n *Allow only* FIPS *Mode* ezarpena aktibatzen denean, DWRCRSA.dll kargatu egiten da ECDH (*Elliptic-curve Diffie-Hellman*) gakoen trukea egiteko. Gakoak trukatzen direnean, bezeroak ECDHren sekretu partekatua sinatzen du EC-ren (*Elliptic Curve)* gako pribatu batekin eta zerbitzarira bidaltzen ditu bai sinadura eta bai ECren gako publikoa, berak sinadura egiaztatu ahal izateko. Gakoen truke mezuaren barnean, autentifikatutako urruneko erasotzaile batek balio handi bat zehatz lezake *SigPubkeyLen* eremuan, DWRCRSA.dll-n bufferraren gainirakurketa/gainidazketa egoera bat sortzeko. Ahultasun horretarako CVE-2020-5734 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Ahultasuna IBMren Log Analysis-en

Argitalpen data: 2020/04/07

Garrantzia: Altua

Kaltetutako baliabideak:

IBM Operations Analytics - Log Analysis, 1.3.1etik 1.3.6ra bitarteko bertsioak.

Azalpena:

IBMk kritikotasun altuko ahultasun bat aurkitu du. Autentifikatu gabeko erasotzaile lokal batek komandoak exekuta litzake sisteman.

Konponbidea:

IBM Operations Analytics - Log Analysys 1.3.6 bertsiora eguneratzea, eta ondoren segurtasun partxea aplikatzea.

Xehetasuna:

Ahultasunaren jatorria da erabiltzailearen sarrera parametroen bidez sistemako komandoak sartzeko aukera.

Etiketak: Eguneraketa, IBM, Ahultasuna

Barneratutako pasahitz erako ahultasuna Dell EMC Data Protection Advisor-en

Argitalpen data: 2020/04/08

Garrantzia: Altua

Kaltetutako baliabideak:

Dell EMC Data Protection Advisor, 6.4, 6.5 eta 18.1 bertsioak.

Azalpena:

DEVCORE-k Dell EMCri eman dio Dell Protection Advisor produktuak duen barneratutako kredentzial erako ahultasun baten berri.

Konponbidea:

Ahultasun hau konpontzeko fabrikatzaileak kaltetutako produktua 18.2, 19.1 edo 19.2 bertsioetara eguneratzea gomendatzen du.

Xehetasuna:

Dell EMC Data Protection Advisor-en hainbat bertsiok ahultasun hau daukate: barneratutako kredentziala kontu ez-dokumentatuan, pribilegio mugatuekin. Autentifikatu gabeko urruneko erasotzaile batek, barneratutako pasahitza zein den jakinez gero, sisteman sar liteke eta irakurketa pribilegioak soilik eskuratu. Ahultasun horretarako CVE-2020-5351 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Informazio konfidentzialera sarbidea VMware-ren vCenter Server-en

Argitalpen data: 2020/04/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

VMware vCenter Server, 6.7 bertsioa, gailu birtualetan edo Windows-en exekutatzen denean.

Azalpena:

VMware-k larritasun kritikoko ahultasun bat aurkitu du. Hori baliatuz urruneko erasotzaile batek informazio konfidentziala ezagutzera eman lezake.

Konponbidea:

6.7u3f segurtasun partxea aplikatzea.

Xehetasuna:

Hainbat baldintzatan, vmdir-ek (VMware Directory Service), VMware vCenter Server-en barnean dagoena, Platform Service Controller (PSC) baten barneratutako edo kanpoko parte modura, ez ditu modu zuzenean inplementatzen sarbide kontrolak, eta hori baliatuz urruneko erasotzaile batek informazio konfidentziala ezagutzera eman lezake. Ahultasun horretarako CVE-2020-3952 identifikatzailea erabili da.

Etiketak: Eguneraketa, VMware, Ahultasuna

Hainbat ahultasun Dell EMCren produktuetan

Argitalpen data: 2020/04/13

Garrantzia: Altua

Kaltetutako baliabideak:

- Dell EMC Data Protection Advisor, 6.4, 6.5 eta 18.1 bertsioak;
- Dell EMC Isilon OneFS, 8.2.2 eta lehenagoko bertsioak.

Azalpena:

Dell EMC produktuek dituzten bi ahultasunen berri eman da, sistema eragilean komandoen injekzio erakoa eta lehenetsitako konfigurazio ez-seguru erakoa. Horiek baliatuz erasotzaile batek sarbidea lor lezake administratzaile modura edo sistema arriskuan jarri.

Konponbidea:

- Dell EMC Data Protection Advisor 18.2, 19.1 edo 19.2 bertsioetara eguneratzea;
- Dell EMC Isilon OneFSren kasuan, 8.2.2 eta lehenagoko bertsioak:
  - NFS desgaitzea,
  - admin home direktorioa mugitzea,
  - Kerberos autentifikazioa gaitzea,
  - SSH pribilegioak kentzea (OneFS web administrazioaren interfazea soilik erabiltzen bada).

Xehetasuna:

- Sistema eragileko komandoen injekzio erako ahultasuna baliatuz, autentifikatutako urruneko erasotzaile batek komando arbitrarioak exekuta litzake kaltetutako sisteman. Ahultasun horretarako CVE-2020-5352 identifikatzailea erreserbatu da.
- Sareko Fitxategien Sistemarako (NFS) Dell Isilon OneFS-k duen lehenetsitako konfigurazioa baliatuz, erasotzaile batek sarbidea lor lezake hasierako 'admin' direktorio batera eta, identifikatzaile bakar (UID) faltsu baten bidez NFSn bitartez, fitxategi konfidentzialak berridatz litzake sistemara sarbide administratiboa eskuratzearren. Ahultasun horretarako CVE-2020-5353 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioen eskalatze erako ahultasuna IBM WebSphere Application Server-en

Argitalpen data: 2020/04/13

Garrantzia: Altua

Kaltetutako baliabideak:

IBM WebSphere Application Server, 7.0, 8.0, 8.5 eta 9.0 bertsioak.

Azalpena:

Pribilegioen eskalatze erako larritasun altuko ahultasun bat dauka IBM WebSphere Application Server-ek.

Konponbidea:

WebSphere Application Server traditional eta WebSphere Application Server Hypervisor Edition-en kasuan, ondoko neurriak ezartzea, kaltetutako bertsioaren arabera:

- 9.0.0.0tik 9.0.5.3ra bitarteko bertsioetarako bi aukera daude:
  - *interim fix-en* eskakizunen arabera eguneratzea eta ondoren *Interim Fix* PH23853 ezartzea,
  - Fix Pack 9.0.5.4 edo geroagokoa ezartzea (2020ko bigarren lauhilekoan eskuragarri).
- 8.5.0.0tik 8.5.5.17ra bitarteko bertsioetarako bi aukera daude:
  - *interim fix-en* eskakizunen arabera eguneratzea eta ondoren *interim fix* PH23853 ezartzea,
  - Fix Pack 8.5.5.18 edo geroagokoa ezartzea (2020ko hirugarren lauhilekoan eskuragarri).
- 8.0.0.0tik 8.0.0.15era bitartean: 8.0.0.15era eguneratzea eta ondoren *Interim Fix* PH23853 aplikatzea.
- 7.0.0.0tik 7.0.0.45era bitartean: 7.0.0.45era eguneratzea eta ondoren *Interim Fix* PH23853 aplikatzea.

Xehetasuna:

IBM WebSphere Application Server ahula da pribilegioen eskalatze baten aurrean *token-ean* oinarritutako autentifikazioa erabiltzen denean administratzaile eskari baten SOAP (*Simple Object Access Protocol*) konektorearen bidez. Ahultasun horretarako CVE-2020-4362 identifikatzailea erabili da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun Palo Alto Networks-en produktuetan

Argitalpen data: 2020/04/13

Garrantzia: Altua

Kaltetutako baliabideak:

- Secdo, Windows-erako bertsio guztiak;
- GlobalProtect Agent, 5.0.8 eta Linux ARMrako 5.1.1 bertsioak baino lehenagokoak;
- PAN-OS, honako bertsioak:
  - 8.1.13 eta 9.0.7 baino lehenagokoak;
  - 9.0.7 baino lehenagokoak LFCdun PA-7000 serieetan.
- Traps, Windowserako 5.0.8 eta 6.1.4 baino lehenagoko bertsioak.

Azalpena:

Palo Alto Networks-en produktuek dituzten hainbat ahultasunen berri eman da. Horiek baliatuz erasotzaile batek pribilegioak eskala litzake, *root* modura sarbidea lortu, *root* modura kodea exekutatu, sistemaren fitxategiak gainidatzi edo zerbitzuaren ukapen egoera eragin.

Konponbidea:

- Secdo-k ez du zerbitzurik. Baina arazoak guztiz arindu daitezke:
  - pribilegiorik ez duten erabiltzaileek fitxategien sistemaren erroan C: edo C:Common izeneko karpeta batean "karpeta sortu" aukerara sarbiderik ez dutela ziurtatuz,
  - C:N-ProgramdataN-SecdoN-Logs karpetaren baimena aldatuz, pribilegiorik ez duten erabiltzaileei sarbidea ez baimentzeko.
- GlobalProtect Agent 5.0.8, 5.1.1 edo bertsio berriagoetara eguneratzea
- PAN-OS 8.1.13, 9.0.7, 9.1.2 edo bertsio berriagoetara eguneratzea.
- Traps 5.0.8, 6.1.4 edo bertsio berriagoetara eguneratzea.

Xehetasuna:

- Secdo script bat exekutatzen saiatzen da kode bide batean. Hori baliatuz, autentifikatutako erabiltzaile lokal batek sistema eragilearen diskoaren errora (C:) sarbidea lor lezake 'karpetak sortu edo datuak gehitu' aukeraren bidez, eta horrela sistemaren pribilegioak eskura litzake bidea existitzen ez bada edo bertan idaztea baimenduta badago. Ahultasun horretarako CVE-2020-1984 identifikatzailea erabili da.
- Secdo-n C:ProgramdataSecdoN-Logs karpetako lehenetsitako baimen okerrak baliatuz, autentifikatutako erasotzaile lokal batek sistemaren fitxategiak gainidatz litzake eta pribilegioak eskalatzea lotu. Ahultasun horretarako CVE-2020-1985 identifikatzailea erabili da.
- GlobalProtect Agent-en aplikazioaren fitxategi zehatzak idazten direnean pribilegioen esleipen desegoki bat baliatuz, autentifikatutako erasotzaile lokal batek root pribilegioak eskura litzake sisteman. Ahultasun horretarako CVE-2020-1989 identifikatzailea erabili da.
- PAN-OS-en kudeaketa zerbitzariko osagaian pilan oinarritutako bufferraren gainezkatze erako ahultasun bat baliatuz, autentifikatutako erabiltzaile batek PAN-OS konfigurazio hondatu bat igo lezake eta kodea exekutatu root pribilegioekin. Ahultasun

horretarako CVE-2020-1990 identifikatzailea erabili da.
- Traps-ek duen aldi baterako fitxategi ez-seguru erako ahultasun bat baliatuz, autentifikatutako erabiltzaile lokal batek pribilegioak eskala litzake edo sistemako fitxategiak gainidatzi. Ahultasun horretarako CVE-2020-1991 identifikatzailea erabili da.
- Erregistroak birbidaltzeko txartela (LFC, Log Forwarding Card) duten PA-7000 serieko gailuetan, PAN-OS-eko Varrcvr deabruak duen formatu kate erako ahultasun bat baliatuz, urruneko erasotzaile batek deabrua blokea lezake zerbitzuaren ukapen egoera sortuz edo kodea exekuta lezake root pribilegioekin. Ahultasun horretarako CVE-2020-1992 identifikatzailea erabili da.

Etiketak: Eguneraketa, Ahultasuna

Intel-en 2020ko apirileko segurtasun buletina

Argitalpen data: 2020/04/15

Garrantzia: Altua

Kaltetutako baliabideak:

- Intel® Modular Server MFS2600KISPP Compute Module, bertsio guztiak;
- Intel® NUC 8 Rugged Kit NUC8CCHKR;
- Intel® NUC Board NUC8CCHB;
- Intel® NUC 7 Essential PC NUC7CJYSAL;
- Intel® NUC Kit NUC7CJYH
- Intel® NUC Kit NUC7PJYH;
- Intel® NUC Kit NUC6CAYS;
- Intel® NUC Kit NUC6CAYH;
- Intel® NUC Kit DE3815TYKHE;
- Intel® NUC Board DE3815TYBE;
- Intel® Compute Stick STCK1A32WFC.

Azalpena:

DCG Red Team-eko Michael N. Henry ikertzaileak eta Dmitry Frolov ikertzaileak 4 ahultasunen berri eman dute, 2 larritasun altukoak eta 2 ertainekoak. Horiek baliatuz erasotzaile batek pribilegioen eskalatzea egin lezake edo zerbitzuaren ukapena eragin.

Konponbidea:

- Intel® Modular Server MFS2600KISPP Compute Module-ren kasuan, fabrikatzaileak gomendatzen du produktua erabiltzeari uztea, zerbitzuz kanpo baitago.
- Intel® NUC eta Intel® Compute Stick-en kasuan, firmware-a azken bertsiora eguneratzea, ohartarazpenaren *Affected Products* taulan azaltzen den moduan.

Xehetasuna:

- Intel(R) Modular Server MFS2600KISPP Compute Module-k duen baldintzen baliozkotze desegokia baliatuz, autentifikatu gabeko alboko erasotzaile batek pribilegioen eskalatzea gaitu lezake. Ahultasun horretarako CVE-2020-0578 identifikatzailea erreserbatu da.
- Intel(R) NUC batzuetarako firmware-ak dituen bufferraren murrizpen desegoki batzuk baliatuz, autentifikatutako erasotzaile lokal batek pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2020-0600 identifikatzailea erreserbatu da.

Larritasun ertaineko ahultasunetarako CVE-2020-0576 eta CVE-2020-0577 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Ahultasuna

Microsoften 2020ko apirileko segurtasun buletina

Argitalpen data: 2020/04/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows;
- Microsoft Edge (EdgeHTMLn oinarritua);
- Microsoft Edge (Edge (Chromium-en oinarritua);
- ChakraCore;
- Internet Explorer;
- Microsoft Office, Microsoft Office Services eta Web Apps;
- Windows Defender;
- Visual Studio;
- Microsoft Dynamics;
- Androiderako Microsoft Apps;
- Mac-erako Microsoft Apps.

Eragina:

Segurtasun eguneraketei buruzko Microsoften apirileko argitalpenean 112 ahultasun jaso dira, 17 kritiko gisa sailkatu dira eta 95 garrantzitsu gisa.

Konponbidea:

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

Xehetasuna:

Argitaratutako ahultasun motak honako hauek dira:

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

Etiketak: Eguneraketa, Microsoft, Nabigatzailea, Ahultasuna, Windows

---

Eguneraketa kritikoak Oracle-n (2020ko apirila)

Argitalpen data: 2020/04/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Application Performance Management, 12.1.0.5, 13.2.0.0, 13.3.0.0 bertsioak;
- Application Service Level Management, 13.2.0.0, 13.3.0.0 bertsioak;
- Enterprise Manager Base Platform, 12.1.0.5, 13.2.0.0, 13.3.0.0 bertsioak;
- Hyperion Financial Management, 11.1.2.4 bertsioa; Enterprise Manager Base Platform, 12.1.0.5, 13.2.0.0, 13.3.0.0 bertsioak;
- Hyperion Financial Reporting, 11.1.2.4 bertsioa;
- Identity Manager Connector, 9.0 bertsioa;
- Instantis EnterpriseTrack, 17.1-17.3 bertsioak;
- Java Advanced Management Console, 2.16 bertsioa;
- JD Edwards EnterpriseOne Tools, 9.2 bertsioa;
- JD Edwards World Security, A9.3, A9.3.1, A9.4 bertsioak;
- MICROS Relate CRM Software, 11.4 bertsioa;
- MySQL Client, 5.6.47 eta lehenagoko bertsioak, 5.7.29 eta lehenagokoak, 8.0.18 eta lehenagokoak;
- MySQL Cluster, 7.3.28 bertsioa eta aurrekoak, 7.4.27 bertsioa eta aurrekoak, 7.5.17 bertsioa eta aurrekoak, 7.6.13 bertsioa eta aurrekoak, 8.0.19 bertsioa eta aurrekoak;
- MySQL Connectors, 5.1.48 eta lehenagoko bertsioak, eta 8.0.19 eta lehenagokoak;
- MySQL Enterprise Monitor, 4.0.11.5331 eta lehenagoko bertsioak, 8.0.18.1217 eta lehenagokoak;
- MySQL Server, 5.6.47 eta lehenagoko bertsioak, 5.7.29 eta lehenagokoak, 8.0.19 eta lehenagokoak;
- MySQL Workbench, 8.0.19 eta lehenagoko bertsioak;
- Oracle Access Manager, 11.1.2.3.0, 12.2.1.3.0 bertsioak;
- Oracle Agile PLM, 9.3.3, 9.3.5, 9.3.6 bertsioak;
- Oracle API Gateway, 11.1.2.4.0 bertsioa;
- Oracle Application Express, 19.2 bertsioa baino lehenagokoak;
- Oracle Application Testing Suite, 13.2.0.1, 13.3.0.1 bertsioak;
- Oracle Banking Enterprise Collections, 2.7.0, 2.8.0 bertsioak;
- Oracle Banking Enterprise Originations, 2.7.0, 2.8.0 bertsioak;
- Oracle Banking Enterprise Product Manufacturing, 2.7.0, 2.8.0 bertsioak;
- Oracle Banking Platform, 2.4.0, 2.4.1, 2.5.0, 2.6.0, 2.6.1, 2.6.2, 2.7.0, 2.7.1, 2.9.0 bertsioak;
- Oracle Big Data Discovery, 1.6 bertsioa;
- Oracle Business Intelligence Enterprise Edition, 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Business Process Management Suite, 12.2.1.4.0 bertsioa;
- Oracle Coherence, 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Communications ASAP Cartridges, 7.2, 7.3 bertsioak;
- Oracle Communications Calendar Server, 8.0.0.2.0, 8.0.0.3.0 bertsioak;
- Oracle Communications Converged Application Server - Service Controller, 6.1 bertsioa;
- Oracle Communications Diameter Signaling Router (DSR), 8.0.0, 8.1.0, 8.2.0, 8.2.1 bertsioak;
- Oracle Communications Element Manager, 8.0.0, 8.1.0, 8.1.1, 8.2.0 bertsioak;
- Oracle Communications Evolved Communications Application Server, 7.1 bertsioa;
- Oracle Communications Messaging Server, 8.0.2 eta 8.1.0 bertsioak;
- Oracle Communications Operations Monitor, 3.4.0, 4.0.0, 4.1.0, 4.2.0, 4.3.0 bertsioak;
- Oracle Communications Service Broker, 6.0, 6.1 bertsioa;
- Oracle Communications Services Gatekeeper, 6.0, 6.1 bertsioak;
- Oracle Communications Session Report Manager, 8.0.0, 8.1.0, 8.1.1, 8.2.0 bertsioak;
- Oracle Communications Session Route Manager, 8.0.0, 8.1.0, 8.1.1, 8.2.0 bertsioak;
- Oracle Communications Unified Inventory Management, 7.3.0, 7.4.0 bertsioak;
- Oracle Communications WebRTC Session Controller, 7.2 bertsioa;
- Oracle Configurator, 12.1, 12.2 bertsioak;
- Oracle Database Server, 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c bertsioak;
- Oracle E-Business Suite, 12.1.1-12.1.3, 12.2.3-12.2.9 bertsioak;
- Oracle Endeca Information Discovery Integrator, 3.2.0 bertsioa;
- Oracle Endeca Server, 7.7.0 bertsioa;
- Oracle Financial Services Analytical Applications Infrastructure, 8.0.6-8.0.9 bertsioak;
- Oracle Financial Services Asset Liability Management, 8.0.6, 8.0.7 bertsioak;
- Oracle Financial Services Balance Sheet Planning, 8.0.8 bertsioa;
- Oracle Financial Services Data Foundation, 8.0.6-8.0.9 bertsioak;
- Oracle Financial Services Deposit Insurance Calculations for Liquidity Risk Management, 8.0.7, 8.0.8 bertsioak;
- Oracle Financial Services Funds Transfer Pricing, 8.0.6, 8.0.7 bertsioak;
- Oracle Financial Services Hedge Management and IFRS Valuations, 8.0.6-8.0.8 bertsioak;
- Oracle Financial Services Liquidity Risk Management, 8.0.6 bertsioa;
- Oracle Financial Services Liquidity Risk Measurement and Management, 8.0.7, 8.0.8 bertsioak;
- Oracle Financial Services Loan Loss Forecasting and Provisioning, 8.0.6-8.0.8 bertsioak;
- Oracle Financial Services Market Risk Measurement and Management, 8.0.6, 8.0.8 bertsioak;
- Oracle Financial Services Price Creation and Discovery, 8.0.7 bertsioa;
- Oracle Financial Services Profitability Management, 8.0.6, 8.0.7 bertsioak;
- Oracle Financial Services Revenue Management and Billing Analytics, 2.6, 2.7, 2.8 bertsioak;
- Oracle FLEXCUBE Core Banking, 4.0 bertsioa;
- Oracle FLEXCUBE Private Banking, 12.0, 12.1 bertsioak;
- Oracle Fusion Middleware MapViewer, 12.2.1.3.0 bertsioa;
- Oracle Global Lifecycle Management NextGen OUI Framework, 12.2.1.3.0, 12.2.1.4.0, 13.9.4.2.2 bertsioak;
- Oracle Global Lifecycle Management OPatch, 11.2.0.3.23 bertsioa baino lehenagokoak, 12.2.0.1.19 baino lehenagokoak, 13.9.4.2.1 baino lehenagokoak;
- Oracle GraalVM Enterprise Edition, 19.3.1, 20.0.0 bertsioak;
- Oracle Health Sciences Information Manager, 3.0 bertsioa;

- Oracle Healthcare Data Repository, 7.0 bertsioa;
- Oracle Hospitality Reporting and Analytics, 9.1.0 bertsioa;
- Oracle HTTP Server, 11.1.1.9.0 bertsioa;
- Oracle In-Memory Performance-Driven Planning, 12.1, 12.2 bertsioak;
- Oracle Insurance Accounting Analyzer, 8.0.6-8.0.9 bertsioak;
- Oracle Java SE, 7u251, 8u241, 11.0.6, 14 bertsioak;
- Oracle Java SE Embedded, 8u241 bertsioa;
- Oracle Knowledge, 8.6.0-8.6.3 bertsioak;
- Oracle Managed File Transfer, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Outside In Technology, 8.5.4, 8.5.5 bertsioak;
- Oracle Real User Experience Insight, 13.1.2.1, 13.2.3.1, 13.3.1.0 bertsioak;
- Oracle Retail Advanced Inventory Planning, 14.0, 15.0, 16.0 bertsioak;
- Oracle Retail Back Office, 14.1 bertsioa;
- Oracle Retail Central Office, 14.1 bertsioa;
- Oracle Retail Customer Management and Segmentation Foundation, 18.0 bertsioa;
- Oracle Retail Merchandising System, 16.0 bertsioa;
- Oracle Retail Order Broker, 15.0, 16.0, 18.0, 19.0 bertsioak;
- Oracle Retail Point-of-Service, 14.1 bertsioa;
- Oracle Retail Predictive Application Server, 15.0.3, 16.0.3 bertsioak;
- Oracle Retail Returns Management, 14.1 bertsioak;
- Oracle Retail Store Inventory Management, 16.0 bertsioa;
- Oracle Retail Xstore Point of Service, 7.1, 15.0, 16.0, 17.0, 18.0, 18.0.1 bertsioak;
- Oracle SD-WAN Edge, 7.3, 8.0, 8.1, 8.2 bertsioak;
- Oracle Secure Backup, 18.1 baino lehenagoko bertsioak;
- Oracle SOA Suite, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Solaris, 10, 11 bertsioak;
- Oracle Transportation Management, 6.3.7, 6.4.2, 6.4.3 bertsioak;
- Oracle Unified Directory, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Utilities Framework, 2.2.0, 4.2.0.2, 4.2.0.3, 4.3.0.2-4.3.0.6, 4.4.0.0, 4.4.0.2 bertsioak;
- Oracle Utilities Network Management System, 1.12.0.3, 2.3.0.1, 2.3.0.2, 2.4.0.0 bertsioak;
- Oracle VM VirtualBox, 5.2.40 baino lehenagoko bertsioak, 6.0.20 baino lehenagokoak, 6.1.6 baino lehenagokoak;
- Oracle WebCenter Portal, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle WebCenter Sites, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle WebLogic Server, 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- OSS Support Tools, 20.0, 20.1 bertsioak;
- PeopleSoft Enterprise CS Campus Community, 9.2 bertsioa;
- PeopleSoft Enterprise HCM Absence Management, 9.2 bertsioa;
- PeopleSoft Enterprise HRMS, 9.2 bertsioa;
- PeopleSoft Enterprise PeopleTools, 8.56, 8.57, 8.58 bertsioak;
- PeopleSoft Enterprise SCM Purchasing, 9.2 bertsioa;
- Primavera Gateway, 16.2.0-16.2.11, 17.12.0-17.12.6, 18.8.0-18.8.8, 19.12.0 bertsioak;
- Primavera P6 Enterprise Project Portfolio Management, 16.2.0.0-16.2.19.3, 17.12.0.0-17.12.17.0, 18.8.0.0-18.8.18.0, 19.12.1.0-19.12.3.0, 20.1.0.0-20.2.0.0 bertsioak;
- Primavera Unifier, 16.1, 16.2, 17.7-17.12, 18.8, 19.12 bertsioak;
- Siebel Applications, 20.2 eta lehenagoko bertsioak;
- StorageTek Tape Analytics SW Tool, 2.3.0 bertsioa;
- Sun ZFS Storage Appliance Kit, 8.8 bertsioa.

Azalpena:

Oraclek partxedun eguneraketa kritiko bat argitaratu du, hainbat produkturi eragiten dieten ahultasunak zuzentzeko.

Konponbidea:

Kaltetutako produktuen arabera, dagozkien partxeak aplikatzea. Eguneraketak deskargatzeko informazioa Oraclek argitaratutako segurtasun buletinean lor daiteke.

Xehetasuna:

Eguneraketa horrek 397 ahultasun konpontzen ditu guztira, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna *Erreferentziak* atalean dagoen Oracle-ren loturan kontsulta daiteke.

Etiketak: Eguneraketa, Oracle, Ahultasuna

Hainbat ahultasunun Aruba-ren ClearPass Policy Manager-en

Argitalpen data: 2020/04/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- ClearPass Policy Manager, 6.8.4 bertsioa baino lehenagoko 6.8.x bertsioak;
- ClearPass Policy Manager, 6.7.13 bertsioa baino lehenagoko 6.7.x bertsioak.

Azalpena:

Luke Young, Sathish eta Darrell Damstedt ikertzaileek 4 ahultasunen berri eman diote Aruba-ri, bat larritasun kritikokoa, beste bat larritasun altukoa eta beste bi larritasun ertainekoak. Autentifikatutako urruneko erasotzaile batek kode arbitrarioa exekuta lezake, pribilegioen eskalatzea egin, informazio konfidentziala ezagutarazi edo segurtasun murrizpenak saihestu eta *cluster*-a arriskuan jarri.

Konponbidea:

- ClearPass Policy Manager, 6.8.x bertsioak 6.8.4 bertsiora eguneratzea;
- ClearPass Policy Manager, 6.7.x bertsioak 6.7.13 bertsiora eguneratzea.

Xehetasuna:

- Larritasun kritikoko ahultasuna baliatuz, ClearPass-en kudeaketa interfazearen sare segmentu berdinean dagoen erasotzaile batek

aldaketak egin litzake ClearPass-en datu base batzuetan, bereziki sortutako HTTP eskaerak bidaliz. Horrela cluster-a guztiz jar lezake arriskuan. Ahultasun horretarako CVE-2020-7114 identifikatzailea erreserbatu da.
- Kritikotasun altuko ahultasunaren jatorria zerbitzariaren aldean dagoen injekzio bat da. Hori baliatuz autentifikatutako erasotzaile batek kodearen urruneko exekuzioa egin lezake. Ahultasun horretarako CVE-2020-7111 identifikatzailea erreserbatu da.
- Larritasun ertaineko ahultasunetarako CVE-2020-7110 eta CVE-2020-7113 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Ahultasuna

SAPen 2020ko apirileko segurtasun eguneraketa

Argitalpen data: 2020/04/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Commerce, 6.6, 6.7, 1808, 1811 eta 1905 bertsioak;
- SAP Diagnostic Agent (LM-Service), 7.20 bertsioa;
- SAP NetWeaver:
  - Knowledge Management, 7.00, 7.01, 7.02, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
  - AS (Application Server) Java (HTTP Service), 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
  - AS ABAP, versiones 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 75A, 75B, 75C, 75D eta 75E bertsioak;
- SAP Business Objects Business Intelligence Platform, 4.1, 4.2 eta 4.3 bertsioak;
- SAP OrientDB, 3.0 bertsioa;
- SAP Solution Manager (Diagnostics Agent), 7.2 bertsioa;
- SAP Host Agent, 7.21 bertsioa;
- SAP Landscape Management, 3.0 bertsioa;
- SAP Adaptive Extensions, 1.0 bertsioa;
- SAP ERP, 618, 730 eta EAPPLGLO 607 bertsioak;
- SAP S/4 HANA, 100, 101, 102, 103, 104, FSAPPL 400, 450, 500 eta S4FPSL 100 bertsioak;
- SAP Business Client, 6.5 eta 7.0 bertsioak;
- SAP Commerce, 1811 eta 1905 bertsioak;
- SAP Fiori Launchpad, 753 eta 754 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 26 segurtasun ohar eman ditu ezagutzera. Horietatik 5 larritasun kritikokoak dira, beste 5 larritasun altukoak eta beste 16 larritasun ertainekoak. Gainera, guztizko 26 ohartarazpenen barnean, lehenagotik argitaratutako segurtasun oharren 3 eguneraketa ere argitaratu dira (2 larritasun kritikokoak eta 1 ertainekoa).

Argitaratutako ahultasun motak honako hauek dira:

- XSS (*Cross-Site Scripting*) erako 11 ahultasun,
- informazio zabalkunde erako 4 ahultasun,
- autentifikazioaren egiaztapen gabeziako 3 ahultasun,
- kodearen injekzio erako 2 ahultasun,
- URLen birbideratze erako 2 ahultasun,
- bideetara kontrolatu gabeko sarbide erako ahultasun bat,
- autentifikazio faltako ahultasun bat;
- XMLren baliozkotze gabeziako ahultasun bat
- beste era batzuetako 8 ahultasun.

Ahultasun horietarako honako identifikatzaileak erabili dira: CVE-2020-6238, CVE-2019-0330, CVE-2020-6225, CVE-2020-6219, CVE-2020-6230, CVE-2020-6235, CVE-2020-6208, CVE-2020-6237, CVE-2020-6234, CVE-2020-6236, CVE-2020-6195, CVE-2020-6212, CVE-2020-6224, CVE-2020-6216, CVE-2020-6215, CVE-2020-6213, CVE-2020-6217, CVE-2020-6229, CVE-2020-6226, CVE-2020-6231, CVE-2020-6222, CVE-2020-6228, CVE-2020-6227, CVE-2020-6232, CVE-2020-6210, CVE-2020-6214 y CVE-2020-6233.

Etiketak: Eguneraketa, SAP, Ahultasuna

Hainbat ahultasun IBM Radar SIEM-en

Argitalpen data: 2020/04/15

Garrantzia: Altua

Kaltetutako baliabideak:

IBM QRadar, 7.3.0 bertsiotik 7.3.3 Patch 2ra bitartekoak.

Azalpena:

IBM QRadar SIEMek dituen fitxategi baimen okerrak eta barneratutako kredentzialak baliatuz, erasotzaile batek pribilegioen eskalatzea egin lezake edo kredentzial horiek erabili.

Konponbidea:

Honako eguneraketak aplikatzea:

- QRadar / QRM / QVM / QNI 7.4.0 GA (SFS);
- QRadar / QRM / QVM / QRIF / QNI 7.3.3 Patch 3 (SFS);
- QRadar / QRM / QVM / QRIF / QNI 7.3.2 Patch 7(SFS);
- QRadar Incident Forensics 7.4.0 (ISO);
- QRadar Incident Forensics 7.4.0 (SFS).

Xehetasuna:

- Fitxategi baimen okerrak baliatuz erasotzaile batek pribilegioen eskalatzea egin lezake. Ahultasun horretarako CVE-2020-4270 identifikatzailea erreserbatu da.
- Barneratutako kredentzialak egotea, esate baterako pasahitz bat edo gako kriptografiko bat, bere sarrera autentifikaziorako, kanpoko osagaietarako irteera komunikaziorako edo barne datuak zifratzeko erabiltzen dena, erasotzaile batek balia lezake kredentzial horiek erabiltzeko. Ahultasun horretarako CVE-2020-4269 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Komandoen injekzioa Dell EMC-ren Integrated Data Protection Appliance-n

Argitalpen data: 2020/04/15

Garrantzia: Altua

Kaltetutako baliabideak:

- Dell EMC Integrated Data Protection Appliance, 2.0, 2.1, 2.2, 2.3 eta 2.4 bertsioak.

Azalpena:

Dell EMC-k larritasun altuko ahultasun bat aurkitu du, Integrated Data Protection Appliance-ri eragiten diona.

Konponbidea:

Dell EMC Integrated Data Protection Appliance 2.5 bertsiora eguneratzea.

Integrated Data Protection Appliance 2.0 bertsioa duten erabiltzaileek lehenbizi 2.1 bertsiora eguneratu beharko dute, ondoren 2.3.1 bertsiora eta azkenik 2.5era.

Xehetasuna:

Komandoen injekzio erako ahultasun bat dago Appliance Configuration Manager osagaian. Autentifikatutako urruneko erasotzaile batek, root pribilegioak izanez gero, komandoak injekta litzake osagai horren APIan eta horrela pasahitzak alda litzake eta komandoak exekutatu. Ahultasun horretarako CVE-2020-5350 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2020/04/16

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- IP Phone 7811, 7821, 7841, 7861, 8811, 8841, 8845, 8851, 8861 y 8865 Desktop Phones;
- Unified IP Conference Phone 8831;
- Wireless IP Phone 8821 eta 8821-EX;
- Cisco UCS Director, honako bertsioak 6.0.0.0, 6.0.0.1, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.0.1.3, 6.5.0.0, 6.5.0.1, 6.5.0.2, 6.5.0.3, 6.5.0.4, 6.6.0.0, 6.6.1.0, 6.6.2.0, 6.7.0.0, 6.7.1.0, 6.7.2.0 eta 6.7.3.0;
- Cisco UCS Director Express for Big Data, 3.7.3.0 eta lehenagoko bertsioak;
- Cisco WLC Software-ren bertsio ahul bat exekutatzen duten Cisco gailuak;
- Mobility Express-en kontrolatzaile modura jarduten duten Cisco Access Points (AP), Cisco WLC Software-ren bertsio ahul bat exekutatzen ari badira;
- Cisco Webex Meetings, WBS 39.5.18 edo WBS 40.2 bertsioak baino lehenagoko Webex Network Recording Player eta Webex Player-en bertsio guztiak;
- Cisco Webex MeetingsOnline, 1.3.48 bertsioa baino lehenagoko Webex Network Recording Player eta Webex Player-en bertsio guztiak;
- Cisco Webex Meetings Server, 4.0MR3 baino lehenagoko Webex Network Recording Player-en bertsio guztiak;
- Aironet 1540/1560/1800/2800/3800/4800 Series Access Points;
- Catalyst IW6300 Access Points;
- 6300 Embedded Services Access Points;
- Cisco IoT Field Network Director, 4.6 baino lehenagoko bertsioak;
- Cisco Unified Communications Manager (UCM) eta Cisco UCM Session Management Edition (SME), 10.5 eta lehenagoko bertsioak, 11.0, 11.5, 12.0 eta 12.5 bertsioak, auto-registration funtzionaltasuna aktibatuta dagoenean.

Azalpena:

Hainbat ikertzailek 18 ahultasun aurkitu dituzte, 11 larritasun kritikokoak eta 7 altukoak, era ezberdinetakoak: kodearen urruneko exekuzioa, zerbitzuaren ukapena, autentifikazio falta, direktorioetara sarbide ez kontrolatua, bufferraren gainezkatzea eta *Cross-Site Request Forgery*.

Konponbidea:

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

Xehetasuna:

Ahultasun horiek baliatuko lituzkeen erasotzaile batek honako ekintzak egin litzake:

- (DoS); kaltetutako gailua berrabiarazi, zerbitzuaren ukapen egoera (DoS) sortuz;
- komando arbitrarioak exekutatu administratzaile pribilegioekin;
- APIari deiak egin;
- kaltetutako sisteman kode arbitrarioa exekutatu;
- fitxategi arbitrarioak irakurri, aldatu edo exekutatu root baimenekin;
- ekintza arbitrarioak egin, esate baterako konfigurazioa aldatzea, kaltetutako erabiltzailearen pribilegio mailarekin;
- (DoS). access point-a (AP) blokeatzea, zerbitzuaren ukapen egoera (DoS) eraginez.

Honako identifikatzaile hauek esleitu dira: CVE-2020-3161, CVE-2020-3239, CVE-2020-3240, CVE-2020-3243, CVE-2020-3247, CVE-2020-3248, CVE-2020-3249, CVE-2020-3250, CVE-2020-3251, CVE-2020-3252, CVE-2016-1421, CVE-2020-3273, CVE-2020-3262, CVE-2020-3194, CVE-2020-3261, CVE-2020-3162, CVE-2020-3177 eta CVE-2020-3260.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Pribilegioen eskalatzea IBMren InfoSphere Information Server-en

Argitalpen data: 2020/04/16

Garrantzia: Altua

Kaltetutako baliabideak:

- InfoSphere Information Server, Information Server on Cloud, 11.7 eta 11.5 bertsioak;
- InfoSphere Information Server, 11.3 bertsioa.

Euren instalazioek ondoko baldintzak betetzen dituztenean:

- Information Server erabiltzen du, 11.7.1 edo lehenagoko bertsioa, edo instalazio hori 11.7.1.0 baino geroagoko bertsio batera eguneratu bada.
- WebSphere Application Server Network Deployment (WAS ND) erabiltzen du.
- 022 baino ahulagoa zen umask erabiliz instalatu zen.

Azalpena:

IBMk kritikotasun altuko ahultasun bat aurkitu du, InfoSphere Information Server-i eragiten diona. Urruneko erasotzaile batek pribilegioen eskalatzea egin lezake.

Konponbidea:

- Modu independentean hedatutako sistemen kasuan:
  - WAS ND kokapenean java karpeta daukan direktorioa aldatu.
  - chmod -R 755 java.
- Klusterretan hedatutako sistemen kasuan:
  - Kudeatzailea instalatuta dagoen makinan:
    - WAS ND kokapenean java karpeta daukan direktorioa aldatu.
    - chmod -R 755 java.
  - Profil pertsonalizatua instalatu zen makinan (hau egin behar da profil pertsonalizatua duten makina guztietan edo klusterreko parte diren makina horizontaletan):
    - WAS ND kokapenean java karpeta daukan direktorioa aldatu.
    - chmod -R 755 java.

Xehetasuna:

IBM InfoSphere Information Server-ek pribilegioen eskalatzean oinarritutako erasoak jasan litzake, WebSphere Application Server Network Deployment-ek erabiltzen dituen fitxategietako baimenen esleipen desegoki baten ondorioz. Ahultasun horretarako CVE-2020-4347 identifikatzailea erreserbatu da.

Etiketak:IBM, Ahultasuna

Segmentazioaren akats erako ahultasuna OpenSSLren SSL_check_chain-en

Argitalpen data: 2020/04/22

Garrantzia: Altua

Kaltetutako baliabideak:

OpenSSL, 1.1.1d, 1.1.1e eta 1.1.1f bertsioak.

Azalpena:

Bernd Edlinger, Matt Caswell eta Benjamin Kaduk ikertzaileek OpenSSLri SSL_check_chain() funtzioan kokatuta dagoen ahultasun baten berri eman zioten, larritasun altukoa eta segmentazioaren akats erakoa.

Konponbidea:

OpenSSL 1.1.1g bertsiora eguneratzea.

Xehetasuna:

SSL_check_chain() funtzioa deitzen duten zerbitzari edo bezero aplikazioak, TLS 1.3 *handshake* egiten ari den bitartean edo ondoren,

blokeatu egin litezke NULL erakuslearen deserreferentzia batengatik, *signature_algorithms_cert* TLS luzapenaren erabilpen oker baten ondorioz. Blokeoa gerta liteke baliagarria edo ezaguna ez den sinadura algoritmo bat jasotzen badu paretik, eta baliatu liteke zerbitzuaren ukapen (DoS) erako eraso bat egiteko. Ahultasun horretarako CVE-2020-1967 identifikatzailea erabili da.

Etiketak: Eguneraketa, SSL/TLS, Ahultasuna

Joomla! 3.9.18ren segurtasun eguneraketa

Argitalpen data: 2020/04/22

Garrantzia: Txikia

Kaltetutako baliabideak:

- Joomla! CMS, honako bertsioak:
  - 3.8.8 tik 3.9.16ra bitartekoak;
  - 2.5.0 tik 3.9.16ra bitartekoak.

Azalpena:

Joomla!-k bi bertsio berri argitaratu ditu, bere nukleoak dituen kritikotasun txikiko 3 ahultasun konpontzen dituena, denak sarbidearen kontrol oker erakoak.

Joomla!-k ez du gomendatzen 3.9.17 bertsiora eguneratzea, eta gomendatzen du zuzenean eguneratzea 3.9.18 bertsiora.

Konponbidea:

3.9.18 bertsiora eguneratzea.

Xehetasuna:

- Sarbidearen Kontrol Zerrendetako (ACL) com_users-en egiaztatze oker bat baliatuz, baimenik gabeko erasotzaile batek erabiltzaileen taldea edita lezake. Ahultasun horretarako CVE-2020-11891 kodea erabili da.
- Erabiltzaileen taldeko taula klasean sarrera parametroen baliozkotze oker batek ACLen konfigurazioa hauts lezake. Ahultasun horretarako CVE-2020-11890 kodea erabili da.
- ACLetako com_users-en egiaztatze oker bat baliatuz, baimenik gabeko erasotzaile batek erabiltzaileen taldea edita lezake. Ahultasun horretarako CVE-2020-11889 kodea erabili da.

Etiketak: eguneraketa, CMS, ahultasuna

Osokoen gainezkatze erako ahultasuna Squid-en

Argitalpen data: 2020/04/24

Garrantzia: Altua

Kaltetutako baliabideak:

- Squid 2.x - 2.7.STABLE9;
- Squid 3.x - 3.5.28;
- Squid 4.x - 4.10;
- Squid 5.x - 5.0.1.

Azalpena:

Osoko zenbakien gainezkatze erako akats baten ondorioz, Squid proxy zerbitzaria ahula da kredentzialen errepikapenaren aurrean eta HTTP Digest-en autentifikazio token-en aurkako urruneko kodearen exekuzio erako erasoen aurrean.

Konponbidea:

Memoriaren *pool*-a erabiltzen denean, arazo hau urruneko bezero batek balia lezake aldez aurretik atzemandako Digest autentifikazio bat erreproduzitzeko, eta horrela sarbidea lortuko luke bestela debekatuta izango lituzkeen baliabideetara. Memoriaren erreserba desgaituta dagoenean, urruneko bezero batek kodea exekuta lezake "free'd nonce" baten kredentzialen bidez. Ahultasun horretarako CVE-2020-11945 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Ahultasuna F5en BIG-IQ Centralized Management-en

Argitalpen data: 2020/04/24

Garrantzia: Altua

Kaltetutako baliabideak: BIG-IQ Centralized Management, 7.0.0, 6.0.0 - 6.1.0, 5.2.0 - 5.4.0 bertsioak.

Azalpena:

Argitaratu den ahultasun baten arabera, erasotzaile batek arriskuan jar litzake BIG-IQren datu batzuk, BIG-IQ HA konfigurazio batean baliatzen denean.

Konponbidea:

7.1.0 bertsiora eguneratzea.

Xahetasuna:

BIG-IQren eskuragarritasun altuko (HA) sinkronizazioa ez da segurua TLS bidez. Hori baliatuz erasotzaile batek iraganbidean dauden datu konfidentzialak irakur/alda litzake. Ahultasun horretarako CVE-2020-5869 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

UDP ataka irekiaren erako ahultasuna HPEren hainbat produktutan

Argitalpen data: 2020/04/24

Garrantzia: Altua

Kaltetutako baliabideak:

- Integrated Maintenance Entity T1805, T1805A01 bertsiotik T1805A01^AAH bertsiora bitartekoak;
- Maintenance Entity T2805, T2805A01 bertsiotik T2805A01^AAU bertsiora bitartekoak;
- Blade Maintenance Entity FW T4805, T4805A01 bertsiotik T4805A01^AAY bertsiora bitartekoak.

Azalpena:

HPE Product Security Response Team-ek larritasun altuko ahultasun bat aurkitu du, UDP ataka ireki bati lotuta. Hori baliatuz erasotzaile batek zerbitzuaren ukapena eragin lezake, informazioa hedatu edo kaltetutako produktuen memoria hondatu.

Konponbidea:

- Integrated Maintenance Entity, T1805A01^AAI bertsiora eguneratzea;
- Blade Maintenance Entity, T4805A01^AAZ bertsiora eguneratzea.

Arintze neurri modura, UDP 17185 ataka blokea daiteke Maintenance LAN Network Switch/Firewall-en.

Xehetasuna:

J/H serieko NonStop sistema guztiek segurtasun ahultasun bat daukate UDP 17185 ataka irekiarekin lotuta Maintenance LANen. Hori baliatuz urruneko erasotzaile batek informazioa zabal lezake, zerbitzuaren ukapen erako (DoS) erasoak egin edo memoria lokala hondatu, eta horrela kaltetutako sistemaren kontrol osoa eskuratuko luke. Ahultasun horretarako CVE-2020-7131 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, HP, Ahultasuna

Hainbat ahultasun IBMren produktuetan

Argitalpen data: 2020/04/24

Garrantzia: Kritikoa

Kaltetutako Baliabideak:

- IBM Spectrum Protect Server, honako bertsioak:
  - 8.1.0.0 bertsiotik 8.1.9.200 bertsiora bitartean;
  - 7.1.0.0 bertsiotik 7.1.10.0 bertsiora bitartean.
- IBM Tivoli Monitoring, 6.3.0 bertsiotik 630 FP7ra bitarteak (*service pack-ak barne*).

Azalpena:

Tenable-ko Chris Lyne ikertzaileak eta Clément Notin ikertzaileak bi ahultasunen berri eman diote IBMri, bat larritasun kritikokoa eta bestea altukoa, bufferraren gainezkatze eta lehenetsitako baimen ez-nahiko erakoak.

Konponbidea:

- IBM Spectrum Protect Server 8.1.9.300 eta 7.1.10.100 bertsioetara eguneratzea.
- IBM Tivoli Monitoring 6.3.0-TIV-ITM-FP0007-CVE-2020-4311 bertsiora eguneratzea.

Xehetasuna:

- IBM Spectrum Protect Server ahula da pilan (stack) oinarritutako bufferraren gainezkatze baten aurrean. Hori baliatuz urruneko erasotzaile batek kode arbitrarioa exekuta lezake sisteman edo kaltetutako produktuaren blokeoa eragin. Ahultasun horretarako CVE-2020-7131 identifikatzailea erabili da.
- IBM Tivoli Monitoring-ek erasotzaile lokal bati ahalbidetu liezaioke bereziki diseinatutako fitxategi bat erabiltzea direktorio berean kokatuta dauden beste DLL fitxategi batzuk kargatzeko. Horrela kode arbitrarioa exekuta lezake kaltetutako produktuan. Ahultasun horretarako CVE-2020-4311 identifikatzailea erabili da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun HPEren zenbait produktutan

Argitalpen data: 2020/04/27

Garrantzia: Altua

Kaltetutako baliabideak:

- HPE IOT GCP, 1.4.0, 1.4.1, 1.4.2 eta 1.2.4.2 bertsioak;
- ProLiant-erako HPE Service Pack, 2018.06.0, 2018.09.0 eta 2018.11.0 bertsioak (Linuxen firmwarearen instalatzaileari soilik aplikatzen zaio);
- HPE SATA Read Intensive Solid State Drives HPG2 (Linuxen firmwarearen instalatzaileari soilik aplikatzen zaio);
- HPE NVMe Mixed Use Solid State Drives HPG2 (Linuxen firmwarearen instalatzaileari soilik aplikatzen zaio);
- HPE Business Critical Hard Drives HPG2 (Linuxen firmwarearen instalatzaileari soilik aplikatzen zaio);
- HPE Server Enterprise Hard Drives HPG2 (Linuxen firmwarearen instalatzaileari soilik aplikatzen zaio);
- HPE Server SAS Hard Drives HPG2 (Linuxen firmwarearen instalatzaileari soilik aplikatzen zaio);
- HPE Server SATA Hard Drives HPG2 (Linuxen firmwarearen instalatzaileari soilik aplikatzen zaio);
- HPE Server Solid State Drives HPG2 (Linuxen firmwarearen instalatzaileari soilik aplikatzen zaio).

Azalpena:

Hiru ahultasun aurkitu dira, 2 larritasun altukoak eta bat ertainekoa, era hauetakoak hurrenez hurren: baimendu gabeko urruneko sarbidea, kode arbitrarioaren exekuzioa modu lokalean, eta informazio sentikorrera urruneko sarbidea.

Konponbidea:

- HPE UIoT 1.4.2 RP204 bertsiora eguneratzea.
- CVE-2020-7135 ahultasunak eragindako produktuen kasuan, konponbideak ohartarazpenaren RESOLUTION atalean ageri dira. Horiek ezar daitezke ProLiant-erako HPE Service Pack 2019.03.0 bertsiora edo berriagoetara eguneratuz, edo Linuxerako Online HDD/SDD Flash Component eguneratuz, biak eskuragarri HPE Support Center-en webgunetik.

Xehetasuna:

- Baimendu gabeko urruneko erasotzaile batek informazio sentikorrera sarbidea eskura lezake HPE UIoT-en hainbat bertsiotan. Ahultasun horretarako CVE-2020-7133 identifikatzailea erabili da.
- Linux exekutatzen duten HPE zerbitzarietan Supplemental Update / Online ROM Flash Component izena duten disko unitateko firmwarearen instalatzaileetan ahultasun bat aurkitu da. Erasotzaile lokal batek kode arbitrarioa exekuta lezake software ahul honetan. Ahultasun horretarako CVE-2020-7135 identifikatzailea erreserbatu da.

Larritasun ertaineko ahultasunerako CVE-2020-7134 identifikatzailea erabili da.

Etiketak: Eguneraketa, HP, Ahultasuna

Sarbidearen kontrol desegokia Fortinet produktuetan

Argitalpen data: 2020/04/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- FortiMail, honako bertsioak:
  - 5.4.10 eta lehenagokoak;
  - 6.0.7 eta lehenagokoak;
  - 6.2.2 eta lehenagokoak.
- FortiVoiceEnterprise, honako bertsioak:
  - 6.0.1 eta lehenagokoak;
  - 5.3 eta lehenagoko bertsioei ahultasunak ez die eragiten.

Azalpena:

Mike Connor ikertzaileak larritasun kritikoko ahultasun bat aurkitu du, sarbidearen kontrol desegoki erakoa, Fortinet-en hainbat produkturi eragiten diena. Autentifikatu gabeko urruneko erasotzaile batek autentifikazioa saihets lezake.

Konponbidea:

- FortiMail honako bertsioetara eguneratzea:
  - 5.4.11 edo geroagokoa;
  - 6.0.8 edo geroagokoa;
  - 6.2.3 edo geroagokoa.
- FortiVoiceEnterprise 6.0.2 edo bertsio berriagoetara eguneratzea.

Xehetasuna:

FortiMail-ek eta FortiVoiceEnterpries-ek duten sarbidearen kontrol desegoki erako ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile bat sistemara sar liteke erabiltzaile zilegizko bat balitz bezala, erabiltzaile interfazearen bidez pasahitz aldaketa eskatuz. Ahultasun horretarako CVE-2020-9294 identifikatzailea erabili da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Bideetara kontrolatu gabeko sarbidea Juniper-en Juno OS-n

Argitalpen data: 2020/04/28

Garrantzia: Altua

Kaltetutako baliabideak:

Junos OS, honako bertsioak: 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4

eta 20.1.

Azalpena:

Juniper-en hainbat produktuk erabiltzen duten HTTP/HTTPS zerbitzuak duen larritasun altuko ahultasun bat baliatuz, autentifikatu gabeko erasotzaile batek fitxategien inklusio lokal bat (LFI, Local File Inclusion) egin lezake edo bideetara kontrolatu gabeko sarbidea lortu.

Konponbidea:

Ahultasun hori konpontzeko softwarearen ondorengo bertsioak argitaratu dira: 12.3X48-D101, 12.3X48-D105, 15.1X49-D211, 15.1X49-D220, 17.4R3-S2, 18.1R3-S10, 18.2R3-S4, 18.3R2-S4, 18.3R3-S2, 18.4R3-S2, 19.1R1-S5, 19.1R3-S1, 19.2R2, 19.3R2-S3, 19.3R3, 19.4R1-S2, 19.4R2, 20.1R1-S1, 20.1R2 eta ondorengo bertsio guztiak, Juniper-en deskargen zentroan eskuragarri.

Xehetasuna:

HTTP/HTTPS zerbitzuak, J-Web, Web Authentication, Dynamic-VPN (DVPN), Web-Redirect erabiltzen duen Firewall Authentication Pass-Through eta Zero Touch Provisioning-ek (ZTP) erabiltzen dutena, ahultasun bat dauka. Hori baliatuz autentifikatu gabeko erasotzaile batek komandoak injekta litzake httpd.log-en, fitxategiak irakurri baimen orokorrekin edo J-Web saio token-ak eskuratu. Ahultasun horretarako CVE-2020-1631 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

XSS ahultasuna VMware ESXi-n

Argitalpen data: 2020/04/29

Garrantzia: Altua

Kaltetutako baliabideak:

VMware ESXi, 6.5 eta 6.7 bertsioak.

Azalpena:

Benny Husted eta DAWUSHIk larritasun altuko ahultasun baten berri eman dute, Cross-Site Scripting (XSS) iraunkor erakoa, VMware ESXi-ren hainbat bertsiotan.

Konponbidea:

- VMware ESXi 6.5, ESXi650-201912104-SG bertsiora eguneratzea;
- VMware ESXi 6.7, ESXi670-202004103-SG bertsiora eguneratzea.

Xehetasuna:

VMware ESXi Host Clientek ez du modu egokian neutralizatzen komandoen sekuentziekin erlazionatutako HTMLa, makina birtualen atributuak ikusten direnean. Erasotzaile batek gonbidatutako sistema eragiletik makina birtual baten sistemaren ezaugarrietara sarbidea balu, asmo gaiztoko script bat injekta lezake, eta hori biktimaren nabigatzaileak exekutatuko luke. Ahultasun horretarako CVE-2020-3955 identifikatzailea erabili da.

Etiketak: Eguneraketa, VMWare, Ahultasuna

Ahultasunak Samban

Argitalpen data: 2020/04/29

Garrantzia: Altua

Kaltetutako baliabideak:

- Todas las versiones de Samba, desde la versión 4.0.0 en adelante;
- Todas las versiones de Samba, desde la versión 4.10.0 en adelante.

Azalpena:

Catalyst-eko Andrew Barlett-ek, eta Andrei Popak bi ahultasun aurkitu dituzte, bat kritikotasun altukoa eta bestea ertainekoa, Sambaren hainbat bertsiori eragiten dietenak. Autentifikatu gabeko urruneko erasotzaile batek aldez aurretik askatutako memoria (use-after-free) erabil lezake edo SIGSEGV bat eragin zerbitzarian.

Konponbidea:

4.10.15, 4.11.8 edo 4.12.2 bertsioetara eguneratzea.

Xehetasuna:

- Larritasun altuko ahultasunaren jatorria autentifikatu gabeko LDAP bilaketa bat da, sakonki habiaratutako iragazki baten bidez. Horrek LDAP zerbitzariaren memoriaren pilaren baliabideak agortu ditzake eta SIGSEGV bat eragin. Ahultasun horretarako CVE-2020-10704 identifikatzailea erreserbatu da.
- Larritasun ertaineko ahultasunerako, aldez aurretik askatutako memoriaren erabilpen erakoa (user-after-free), CVE-2020-10700 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Samba, Ahultasuna

Baimenik gabeko urruneko sarbidea HPEren Smart

Update Manager-en

Argitalpen data: 2020/04/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Smart Update Manager (SUM), 8.5.6 bertsioa baino lehenagokoak.

Azalpena:

HPEren SUM produktuek dituzten larritasun kritikoko hiru ahultasun argitaratu dira, baimenik gabeko urruneko sarbidea ahalbidetu lezaketenak.

Konponbidea:

SUMen azken bertsiora eguneratzea HPEren zerbitzu zentrotik.

Xehetasuna:

HPEren Smart Update Manager-ek dituen larritasun kritikoko hiru ahultasun baliatuz erasotzaile batek baimendu gabeko urruneko sarbidea lor lezake. Ahultasun horietarako ondoko identifikatzaileak esleitu dira: CVE-2017-2921 eta CVE-2017-2922. Eta CVE-2020-7136 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, HPE, Ahultasuna

Komandoen injekzioa Cisco-ren IOS XE SD-WAN-en

Argitalpen data: 2020/04/30

Garrantzia: Altua

Kaltetutako baliabideak:

IOS XE SD-WAN softwarea exekutatzen duten Ciscoren ondoko gailuak::

- 1000 Series Aggregation Services Routers,
- 1000 Series Integrated Services Routers (ISRs),
- 4000 Series ISRs,
- Cloud Services Router 1000V Series.

Azalpena:

Synacktiv-eko Julien Legras eta Thomas Etrillard ikertzaileek kritikotasun altuko ahultasun bat aurkitu dute, Ciscoren hainbat gailuri eragiten diena. Autentifikatutako erasotzaile lokal batek komandoak injekta litzake root pribilegioekin.

Konponbidea:

Aipatutako ahultasuna konpontzen duten eguneraketak Software Ciscoren deskarga paneletik deskarga daitezke.

Xehetasuna:

Ahultasunaren jatorria sarrera parametroen baliozkotze ez-nahikoa da. Autentifikatutako erasotzaile lokal batek bereziki sortutako sarrera bat sar lezake CLI utilitatean, eta gailuan komandoak exekuta litzake root pribilegioekin. Ahultasun horretarako CVE-2019-16011 identifikatzailea erabili da.

Etiketak: Aguneraketa, Cisco, Ahultasuna

WordPress-entzat 5.4.1 segurtasun eguneraketa

Argitalpen data: 2020/04/30

Garrantzia: Altua

Kaltetutako baliabideak:

WordPress, 5.4 eta lehenagoko bertsioak.

Azalpena:

WordPress-en azken bertsioa argitaratu da, 7 segurtasun arazo zuzentzen dituena.

Konponbidea:

- 5.4.1 bertsiora eguneratzea,
- 3.7 bertsioaz geroztikako WordPress-en bertsio guztiek daukate eguneraketa eskuragarri.

Xehetasuna:

Segurtasun zuzenketek ondoko ahultasunak konpontzen dituzte, erasotzaile bati honakoa egitea ahalbidetuko lioketenak:

- argitaratu gabeko edukiak ikustea baimenik gabe,
- pasahitzen token-en berrabiatzean akatsa,
- Cross-site scripting erako eraso bat Customizer-en,

- Cross-site scripting erako eraso bat bilaketen koadroan,
- Cross-site scripting erako eraso bat wp-object-cache-n,
- Cross-site scripting erako eraso bat fitxategien igoeran,
- gordetako Cross-site scripting erako eraso bat WordPress customizer-en,
- Cross-site scripting erako eraso bat block editor-en.

Etiketak: Eguneraketa, CMS, Ahultasuna

Hainbat ahultasun F5 produktuetan

Argitalpen data: 2020/04/30

Garrantzia: Altua

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), honako bertsio hauek:
  - 11.6.1 bertsiotik 11.6.5 bertsiora bitartekoak;
  - 12.1.0 bertsiotik 12.1.5 bertsiora bitartekoak;
  - 13.1.0 bertsiotik 13.1.3 bertsiora bitartekoak;
  - 14.0.0 bertsiotik 14.1.2 bertsiora bitartekoak;
  - 15.0.0 bertsiotik 15.0.1 bertsiora bitartean, eta 15.1.0.
- BIG-IQ Centralized Management, honako bertsioak:
  - 5.3.0 bertsiotik 5.4.0 bertsiora bitartekoak;
  - 6.0.0 bertsiotik 6.1.0 bertsiora bitartekoak;
  - 7.0.0 bertsiotik 7.1.0 bertsiora bitartekoak.

Azalpena:

8 ahultasun aurkitu dira F5en hainbat produktutan, guztiak larritasun altukoak, era hauetakoak: zifratuen erabilpena backend zerbitzarietan, hardware-aren azelerazio kriptografikoan akatsa, scp (secure copy) bidez asmo gaiztoko eskaeraren bidalketa, bereziki diseinatutako eskaeren bidalketa zerbitzari birtual batera, nukleoaren fitxategia sortzea eta TMM (Traffic Management Microkernel) berrabiatzea, sinkronizazio peer berri batera zifratu gabeko konexio saioak, gaizki sortutako sarrera datuak eta ustekabeko IP trafikoaren prozesamendua.

Konponbidea:

BIG-IP ondoko bertsioetako batera eguneratzea:

- 11.6.5.1,
- 12.1.5, 12.1.5.1;
- 13.1.3.2,
- 14.0.1.1, 14.1.2.4;
- 15.0.0, 15.0.1.1, 15.0.1.2, 15.0.1.3, 15.1.0, 15.1.0.2.

Xehetasuna:

Erabiltzaile batek aipatutako ahultasunak baliatuko balitu, kaltetutako produktuetan honako ekintza hauek egin litzake:

- zerbitzuaren ukapena (DoS),
- akatsengatik kommutazio gertakaria (failover event),
- komando arbitrarioen exekuzioa pribilegio altuekin,
- zerbitzua etetea,
- trafikoaren fluxua etetea, akatsengatik kommutazio bat sortuz (failover) itxaroten dagoen sistema batera,
- sisteman informazio sentikorra eskuratu edota aldatu,
- akatsa trafikoa prozesatzean.

Ahultasun horietarako CVE-2020-5871, CVE-2020-5872, CVE-2020-5873, CVE-2020-5874, CVE-2020-5875, CVE-2020-5876, CVE-2020-5877 eta CVE-2020-5878 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Ahultasuna