2019ko Maiatzaren Bulletina

Ohartarazpenak - Teknikoak

Ahultasuna Citrix-en SD-WAN Appliance-n

Argitalpen data: 2019/05/02

Garrantzia: Handia

Kaltetutako baliabideak:

- Honakoen bertsio guztiak:
  - NetScaler SD-WAN 9.x
  - NetScaler SD-WAN 10.0.x, 10.0.7 baino lehenagokoak
  - Citrix SD-WAN 10.1.x
  - Citrix SD-WAN 10.2.x, 10.2.2 baino lehenagokoak

Azalpena:

SD-WAN New Hop(e)-ko Sergey Gordeychik, Denis Kolegov eta Nikita Oleksov ikertzaileek, Citrix-ekin lankidetzan, kritikotasun altuko ahultasun bat aurkitu dute. Hori baliatuz erasotzaile batek *man-in-the-middle* erako eraso bat egin lezake.

Konponbidea:

Citrix-ek ahultasuna arintzen duten hainbat eguneraketa argitaratu ditu, kaltetutako produktuaren eta bertsioaren arabera:

- NetScaler SD-WAN 10.0.7 bertsiora eguneratzea
- Citrix SD-WAN 10.2.2 bertsiora eguneratzea

Erabiltzaile erregistratuek eguneraketak Citrix-en deskargen zentroan eskura ditzakete.

Xehetasuna:

- Citrix SD-WAN Appliance-k duen informazioaren hedapen erako ahultasuna baliatuz, autentifikatu gabeko erasotzaile batek man-in-the-middle erako eraso bat egin lezake trafikoaren kudeatzailearen aurka. Ahultasun horretarako CVE-2019-11550 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Zerbitzuaren ukapen erako ahultasuna F5en produktuetan

Argitalpen data: 2019/05/02

Garrantzia: Handia

Kaltetutako baliabideak:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), ondoko bertsioak:
  - 14.0.0tik 14.1.0ra bitartekoak
  - 13.0.0tik 13.1.1era bitartekoak
  - 12.1.0tik 12.1.4ra bitartekoak
  - 11.6.1etik 11.6.3ra bitartekoak
  - 11.5.1etik 11.5.8ra bitartekoak

Azalpena:

F5ek bere produktu batzuei eragiten dieten larritasun altuko bi ahultasunen berri eman du. Ahultasun horiek arrakastaz baliatuz gero, zerbitzuaren ukapen egoera (DoS) sor liteke, TMM (Trafic Management Microkernel) berrabiatzea eraginez.

Konponbidea:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), ondoko bertsioak:
  - 14.0.0tik 14.1.0ra bitartean, 14.1.0.2ra eguneratzea
  - 13.0.0tik 13.1.1era bitartean, 13.1.1.5era eguneratzea
  - 12.1.0tik 12.1.4ra bitartean, 12.1.4.1era eguneratzea
  - 11.6.1etik 11.6.3ra bitartean, 11.6.4ra eguneratzea
  - 11.5.1etik 11.5.8ra bitartean, 11.5.9ra eguneratzea

Xehetasuna:

- Bi ahultasunetako batek BIG-IP zerbitzari birtualari eragiten dio, TCP eta DNS profila baldin badu eta gainera DNSren cache memoria gaituta baldin badu. DNS kontsulten TCP konexioak bertan behera uzten badira DNS cachearen erantzuna jaso aurretik, zerbitzuaren ukapen egoera (DoS) sor liteke, TMMren berrabiatzea eragitean. Ahultasun horretarako CVE-2019-6612 identifikatzailea erreserbatu da.
- Beste ahultasuna VPN PPTP trafikoan gertatzen diren datuen sekuentzia arraro batzuk prozesatzean ematen da. Horrek TMM berrabiatzea eragin lezake, eta ondorioz zerbitzuaren ukapen egoera (DoS) gerta liteke. Ahultasun horretarako CVE-2019-6611 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/05/02

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Nexus 9000 Series Fabric Switches, Application Centric Infrastructure (ACI) moduan.
- Cisco Web Security Appliance-rako Cisco AsyncOS Software, bai gailu birtualetan eta bai hardware gailuetan.
- Cisco Umbrella Dashboard.
- 3000 Series Industrial Security Appliances (ISAs).
- Adaptive Security Appliance (ASA):
  - 1000V Cloud Firewall.
  - 5505 Series Adaptive Security Appliance (ASA 5505-en ezberdinak diren ASA 5500 Series Adaptive Security Appliances direnak zerbitzuaren epearen amaierara iritsi dira eta dagoeneko ez dira ebaluatzen segurtasun ahultasunei dagokienez).
  - 5500-X Series Firewalls.
  - Cisco Catalyst 6500 Series Switches eta Cisco 7600 Series Routers-erako Services Module.
  - FirePOWER Services-dun 5500-X Series.
- Adaptive Security Virtual Appliance (ASAv).
- Firepower:
  - 2100 Series.
  - 4100 Series.
  - 9300 ASA Security Module.
  - Threat Defense Virtual.
  - 7000 Series Appliances.
  - 8000 Series Appliances.
  - 9300 Security Appliances.
- Produktu hauen 1.4.10.6 bertsioa baino lehenagokoak:
  - Small Business 200 Series Smart Switches.
  - Small Business 300 Series Managed Switches.
  - Small Business 500 Series Managed Switches.
- Produktu hauen 2.5.0.78 bertsioa baino lehenagokoak:
  - 250 Series Smart Switches.
  - 350 Series Managed Switches.
  - 350X Series Managed Switches.
  - 550X Series Stackable Managed Switches.
- Cisco Small Business RV320 eta RV325 Dual Gigabit WAN VPN Routers, 1.4.2.20 baino lehenagoko firmware bertsioak.
- IP Conference Phone 7832 eta 8832
- IP Phone 7811, 7821, 7841, 7861, 8811, 8841, 8845, 8851, 8861 eta 8865
- Unified IP 8831 Conference Phone (beretzako konponbidea 2019 amaierarako aurreikusita dago) eta Third-Party Call Control-erako Unified IP 8831 Conference Phone (oraindik konponbiderik gabe).
- Wireless IP Phone 8821 eta 8821-EX.
- Networks-erako Advanced Malware Protection (AMP) honakoetan:
  - FirePOWER 7000 Series Appliances.
  - FirePOWER 8000 Series Appliances.
  - FirePOWER 9300 Series Appliances.
- Integrated Services Routers-erako (ISRs) Firepower Threat Defense.
- FTD Virtual (FTDv).
- Next-Generation Intrusion Prevention System (NGIPS).
- Cisco ASA Software-ren bertsio ahul bat exekutatzen duten eta web kudeaketarako sarbidea gaituta duten Cisco produktuak.
- Cisco Application Policy Infrastructure Controller (APIC) Software, 4.1(1i) baino lehenagoko bertsioak.
- Cisco Nexus 9000 Series ACI Mode Switch Software, 14.1(1i) baino lehenagoko bertsioak.

Azalpena:

Ciscok 22 ahultasunen berri eman du, horietatik 1 larritasun kritikokoa eta gainerakoak larritasun altukoak.

Konponbidea:

- Ciscok ahultasunak konpontzen dituzten eguneraketak argitaratu ditu, kaltetutako produktuaren arabera. Eguneraketak

eskuragarri daude Ciscoren softwarearen deskargen panelean.

Xehetasuna:

Ahultasunak ondoren aipatzen dira, bakoitzarentzat erreserbatutako identifikatzaile eta guzti:

- SSH gakoen kudeaketan akatsa: CVE-2019-1804.
- Pribilegioen eskalatzea: CVE-2019-1816, CVE-2019-1803, CVE-2019-1682 eta CVE-2019-1592.
- Zerbitzuaren ukapena: CVE-2019-1817, CVE-2018-15388, CVE-2019-1635, CVE-2019-1696, CVE-2019-1704, CVE-2019-1703, CVE-2018-15462, CVE-2019-1706, CVE-2019-1708, CVE-2019-1693 eta CVE-2019-1694.
- Saioen kudeaketaren funtzionaltasunean akatsa: CVE-2019-1807.
- Autentifikazioari ihes egitea: CVE-2019-1859 eta CVE-2019-1714.
- Saioaren bahiketa: CVE-2019-1724.
- Entropia ez-nahikoa gako kriptografikoak sortzean: CVE-2019-1715.
- Cross-Site Request Forgery (CSRF): CVE-2019-1713.
- TLS bezeroaren autentifikazio ez-segurua: CVE-2019-1590.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun SAP produktuetan

Argitalpen data: 2019/05/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP S/4HANA®
- SAP Enterprise Resource Planning (ERP)
- SAP Product Lifecycle Management (PLM)
- AP Customer Relationship Management (CRM)
- SAP Human Capital Management (HCM)
- SAP Supply Chain Management (SCM)
- SAP Supplier Relationship Management (SRM)
- SAP NetWeaver® Business Warehouse (BW)
- SAP Business Intelligence (BI)
- SAP Process Integration (PI)
- SAP Governance
- SAP Solution Manager (SolMan)
- Risk & Compliance 10.x (GRC)
- SAP NetWeaver ABAP® Application Server 7.0 - 7.52

Azalpena:

Dubain 2019ko apirilean egindako OPCDE Security Conferencen hainbat ahultasunen berri eman da, *10KBLAZE* izeneko konfigurazio akatsei lotutakoak, eta larritasun kritikokoak direnak. Ahultasun horiek hainbat SAP aplikazio jar ditzakete arriskuan, eta baita negozio aplikazioaren datu guztiak ezabatu ere, edo informazio sentikorra aldatu eta atera.

Ahultasun horiek aurkitu eta partxeatu zituen SAPek 2005, 2009 eta 2019an. Baina konfigurazio akats horiek ezagutzen direnez, aktiboki balia daitezkeenez, eta beren kritikotasuna dela eta, SAPen aholkuak jarraitzea gomendatzen da sistemen instalazioak eta eguneraketak egiterakoan.

Konponbidea:

- SAPen segurtasun oharrak ezarri: #821875 (2005), #1408081 (2009) eta #1421005 (2010). SAP bezeroek oharren edukira sarbidea lor dezakete SAPen laguntza atariaren bidez (autentifikazioa behar da).
- Suebakietan eta IPS/IDS gailuetan detektatze funtzioak ezartzea Snort-en sinadura arauekin. Suebakien hornitzaile aitortuentzako sinadurak publiko egin dira, hala nola Cisco, FireEye eta Palo Alto.

Xehetasuna:

- Azaldutako ahultasunak SAP Netweaver instalazioek duten konfigurazio administratiboko akatsengatik gertatzen dira, horiek ez badira egin SAPek eskainitako aholkuekin.
- Ahalik azkarren neurriak hartzea gomendatzen da, konfigurazio akats horiek ezagunak baitira eta aktiboki erabiliak izan litezke.

Etiketak: Eguneraketa, SAP, Ahultasuna

XXE erako ahultasuna IBM TRIRIGAn

Argitalpen data: 2019/05/06

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM TRIRIGA Application Platform, 3.5.3 eta 3.6.0 bertsioak

Azalpena:

XXE (XML External Entity) injekzio erako ahultasuna dago IBM TRIRIGA Application Platform-en.

Konponbidea:

- IBM TRIRIGA Application Platform-en partxeak aplikatzea, 3.5.3.6 eta 3.6.0.3 bertsioak.

Xehetasuna:

- IBM TRIRIGA es vulnerable a un ataque XXE (*XML External Entity*) al procesar datos XML. Un atacante remoto podría aprovechar

esta vulnerabilidad para exponer información confidencial o consumir recursos de memoria. Se ha reservado el identificador CVE-2019-4208 para esta vulnerabilidad.

Etiketak: Eguneraketa, IBM, Ahultasuna

Hainbat ahultasun PrinterLogic-en Print Management Softwaren

Argitalpen data: 2019/05/06

Garrantzia: Handia

Kaltetutako baliabideak:

- PrinterLogic, 18.3.1.96 bertsioa eta lehenagokoak

Azalpena:

PrinterLogic Print Management softwareak ez ditu baliozkotzen SSL eta softwarea eguneratzeko ziurtagiriak. Hori baliatuz, erasotzaile batek softwarea birkonfigura lezake, eta urrunetik kodea exekutatu. Gainera, PrinterLogic agenteak ez du baliozkotzen nabigatzailearen sarrera, eta hori baliatuz, urruneko erasotzaile batek konfigurazioa alda lezake. Ahultasun hauen ondorioz urrunetik kodea exekuta liteke PrinterLogic agentea exekutatzen duten lan estazioetan.

Konponbidea:

- PrinterLogic eguneratzea partxeak eskuragarri daudenean.
- VPNren erabilpena aztertzea MITM agertokiak saihesteko, eta aplikazioen zerrenda zuriak aplikatzea PrinterLogic agenteak asmo gaiztoko koderik exekuta ez dezan

Xehetasuna:

- PrinterLogic Print Management softwareak ez du baliozkotzen, edo modu okerrean baliozkotzen du PrinterLogic-en kudeaketa atariaren SSL ziurtagiria. Ziurtagiri bat baliogabea edo asmo gaiztokoa denean, erasotzaile batek konfiantzazko entitate bat ordeztea ahalbidetu dezake Man In *The Middle* (MITM) erako eraso bat erabiliz. Softwarea asmo gaiztoko host batera konekta daiteke konfiantzazko host bat dela pentsatuz, edo engainatua izan daiteke ustez konfiantzazko host batetik datozen datuak onar ditzan. Ahultasun horretarako CVE-2018-5408 identifikatzailea erreserbatu da.
- PrinterLogic Print Management softwareak kodea eguneratu eta exekutatzen du, bere jatorria edo integritatea aski egiaztatu gabe. Erasotzaile batek asmo gaiztoko kodea exekuta lezake eta host zerbitzaria arriskuan jarri, *spoofing* DNS eginez edo iraganbideko kodea aldatuz. Ahultasun horretarako CVE-2018-5409 identifikatzailea erreserbatu da.
-
- PrinterLogic Print Management softwareak ez ditu garbitzen karaktere bereziak, eta ondorioz urrunetik baimenik gabeko aldaketak egin daitezke konfigurazio fitxategietan. Ahultasun horretarako CVE-2019-9505 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Pribilegioen eskalatze erako ahultasuna IBM InfoSphere Information Server-en

Argitalpen data: 2019/05/07

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM InfoSphere Information Server, 11.7.1 bertsioa
- IBM InfoSphere Information Server on Cloud, 11.7.1 bertsioa

Azalpena:

Pribilegioen eskalatze erako ahultasuna aurkitu da IBM InfoSphere Information Server-en.

Konponbidea:

- IBMk ez du oraindik konponbiderik argitaratu ahultasun honetarako. Nolanahi ere, fabrikatzailearen ohartarazpeneko *Workarounds and Mitigations* atalean azaltzen diren urratsak jarrai daitezke lan eremua segurua izan dadin lortzeko.

Xehetasuna:

- IBM InfoSphere Information Server-en edukitzaileak ahulak dira pribilegioen eskalatze erako eraso baten aurrean, modu ez-seguruan konfiguratutako osagai bat dela eta. Ahultasun horretarako CVE-2019-4185 identifikatzailea erreserbatu da

Etiketak: 0day, IBM, Ahultasuna

Joomla! 3.9.6ren segurtasun eguneraketa

Argitalpen data: 2019/05/08

Garrantzia: Txikia

Kaltetutako baliabideak:

- Joomla! CMS, 1.7.0tik 3.9.5era bitarteko bertsioak

Azalpena:

Joomla!-k bertsio berri bat argitaratu du, nukleoak duen kritikotasun txikiko ahultasun bat konpontzen duena. Ahultasun hori *cross-site scripting* (XSS) erakoa da.

Konponbidea:

- 3.9.6 bertsiora eguneratzea.

Xehetasuna:

- *com_users-en* arazketa ikuspegiek ez zituzten modu zuzenean garbitzen erabiltzaileak emandako datuak, eta horren ondorioz XSS eraso bat egin liteke. Ahultasun horretarako CVE-2019-11809 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, CMS, Ahultasuna

Autentifikazioaren jauzi erako ahultasuna Cisco Elastic Services Controller-en

Argitalpen data: 2019/05/08

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco Elastic Services Controller, sofwarearen 4.1, 4.2, 4.3 edo 4.4 bertsioak exekutatzean, REST API gaituta dutenean.

Azalpena:

Cisco Elastic Services Controller-en (ESC) larritasun kritikoko ahultasun bat aurkitu dute. Hori baliatuz autentifikaziorik gabeko urruneko erasotzaile batek autentifikazioa saihets lezake REST APIn eta sisteman ekintzak egin.

Konponbidea:

- Ciscok ahultasuna arintzen duen eguneraketa bat argitaratu du, softwarearen bertsioaren arabera. Bere softwarearen deskarga zentrotik jaits daiteke.
- Kaltetutako bertsioak:
  - 4.1 bertsioa honako bertsioetara eguneratzea:
    - 4.1.0.100
    - 4.1.0.111
  - 4.2 bertsioa honako bertsioetara eguneratzea:
    - 4.2.0.74
    - 4.2.0.86
  - 4.3 bertsioa honako bertsioetara eguneratzea:
    - 4.3.0.121
    - 4.3.0.128
    - 4.3.0.134
    - 4.3.0.135
  - 4.4 bertsioa honako bertsioetara eguneratzea:
    - 4.4.0.80
    - 4.4.0.82
    - 4.4.0.86
- 4.5 bertsioak eta 4.1 baino lehenagokoek ez dute kalterik.

Xehetasuna:

- Ahultasunaren arrazoia APIra bidalitako eskaeretan egiten den baliozkotze okerra da. Erasotzaile batek ahultasun hori balia lezake REST APIra bereziki sortutako eskari bat bidaliz. Horren ondorioz, erasotzaileak ekintzak exekuta litzake REST APIaren bidez administratzaile pribilegioekin kaltetutako sisteman. Ahultasun horretarako CVE-2019-1867 identifikatzailea erreserbatu da.

Etiketak: ***Eguneraketa, Cisco, Ahultasuna***

Hainbat ahultasun HPEren Intelligent Management Center-en

Argitalpen data: 2019/05/10

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Intelligent Management Center.

Azalpena

Incite Team-eko Matthias Kaiser eta Steven Seeley-ek 8 ahultasunen berri eman dute, horietatik bat larritasun ertainekoa, 5 altukoak eta 2 kritikoak. Azaldutako ahultasunak baliatuz kodearen urruneko exekuzio erako eta kredentzial kriptografikoen zabalpen erako erasoak egin litezke.

Konponbidea

- Oraindik ez dago eguneraketarik ahultasun horiek konpontzeko. Arintze neurri modura, zerbitzuarekiko interakzioa konfiantzako makinei soilik baimentzea aholkatzen da. Zerbitzuarekin prozesu harreman zilegi bat duten bezero eta zerbitzariak soilik

komunikatu ahal izan behar dira berarekin. Hori hainbat eratara lor liteke, batez ere *firewall-ean* arauak jarriz edo zerrenda zuriekin.

Xehetasuna

Larritasun kritikoko ahultasunak honako hauek dira:

- Akats zehatz bat dago *AccessMgrServlet endpoint-ean*. Eskariak aztertzean, prozesuak ez ditu zuzen egiaztatzen erabiltzaileak emandako datuak, eta horrek datu ez fidagarrien deserializazioa eragin dezake. Erasotzaile batek ahultasunak balia litzake kode arbitrarioa exekutatzeko SYSTEM testuinguruan.
- Akats bat gertatzen da AMF3 eskaeren maneiuan *amf endpoint-eraino*. Arazoaren arrazoia da erabiltzaileak emandako datuak ondo ez baliozkotzea, eta horrek datu ez-fidagarrien deserializazioa eragin dezake. Erasotzaile batek ahultasunak balia litzake kode arbitrarioa exekutatzeko SYSTEM testuinguruan.

Etiketak: 0day, HP, Ahultasuna

XML External Entity erako ahultasuna IBM i2 Intelligence Analysis Platform-en

Argitalpen data: 2019/05/10

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM i2 Analyst's Notebook 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.0.4, 9.0.5, 9.0.6, 9.0.7, 9.1.0 eta 9.1.1
- IBM i2 Analyst's Notebook Premium 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.0.4, 9.0.5, 9.0.6, 9.0.7, 9.0.8, 9.1.0 eta 9.1.1
- IBM i2 Enterprise Insight Analysis

Azalpena:

IBM i2 Intelligent Analyis Platform-ek XXE (XML External Entity) erako ahultasun bat konpondu du. Hori baliatuz erasotzaileek informazio konfidentzialera sarbidea eskura lezakete, edo erabiltzailearen sistemak urruneko zerbitzarietara deiak egitea eragin lezakete:

Konponbidea:

- IBM i2 Analyst's Notebook Version 9.0.6
- IBM i2 Analyst's Notebook Version 9.1.1
- IBM i2 Analyst's Notebook Premium Version 9.06
- IBM i2 Analyst's Notebook Premium Version 9.1.1

Kaltetutako gainerako bertsioetarako partxerik ez dag, eta ondorioz aurreko bertsioetara eguneratzea gomendatzen da.

Xehetasuna:

- IBM i2 Intelligent Analyis Platform-ek ahultasuna dauka XML (XXE) kanpoko entitatearen injekzio erako eraso baten aurrean XML datuak prozesatzean. Urruneko erasotzaile batek ahultasun hori balia lezake informazio sentikorra agerian uzteko edo memoriaren baliabideak kontsumitzeko. Ahultasun horretarako CVE-2019-4062 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Kodearen urruneko exekuzioaren erako ahultasuna SQLite-n

Argitalpen data: 2019/05/10

Garrantzia: Handia

Kaltetutako baliabideak:

- SQLite, 3.26.0 eta 3.27.0 bertsioak

Azalpena:

Cisco Talos-eko Cory Duplantis ikertzaileak aurkitu duenez, SQLitek memoriaren askapenaren ondoreneko erabilera erako ahultasun bat dauka, eta hori baliatuz gero, erasotzaile batek urrunetik kodea exekutatzeko ahalmena lor lezake xede den ekipoan.

Konponbidea:

- SQLite-k, Cisco Talos-ekiko lankidetzan, eguneraketa bat argitaratu du kaltetutako bezeroentzat, beren deskargen orrian eskura daitekeena.

Xehetasuna:

- SQLite-k SQLren Window Functions ezaugarria dauka, lerroen azpimultzo edo window baten gainean kontsultak egitea ahalbidetzen duena. Ahultasun zehatz hau window funtzioan dago. Bereziki diseinatutako SQL komando batek memoriaren askapenaren ondoreneko erabilera erako ahultasun bat sor lezake, eta horrek kodearen urruneko exekuzioa eragin lezake. Ahultasun horretarako CVE-2019-5018 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Cross-Site Scripting (XSS) iraunkorra Liferay-n

Argitalpen data: 2019/05/13

Garrantzia: Handia

Kaltetutako baliabideak:

- com.liferay.faces.alloy-2.0.0 (Liferay Portal 6.2)
- com.liferay.faces.alloy-2.0.1 (Liferay Portal 6.2)
- com.liferay.faces.alloy-3.0.0 (Liferay Portal 7.0)
- com.liferay.faces.alloy-3.0.1 (Liferay Portal 7.0)
- liferay-faces-alloy-3.2.5-ga6 (Liferay Portal 6.2)
- liferay-faces-alloy-4.2.5-ga6 (Liferay Portal 6.2)

Azalpena:

Liferay Faces Alloy-ren bertsio batzuek duten Cross-Site Scripting (XSS) iraunkor erako ahultasun baten berri argitaratu da.

Konponbidea:

- Kaltetutako bertsioaren arabera partxe egokia aplikatzea.

Xehetasuna:

- Cross-Site Scripting (XSS) iraunkor erako ahultasun bat dago *alloy:autoComplete* eta *alloy:inputFile-n*. Horren arrazoia da Liferay Faces Alloy-ren bertsio kaltetuen array-etan JavaScript kateen errepresentazio oker bat.

Etiketak: Eguneraketa, Ahultasuna

Vulnerabilidad en la funcionalidad pingback de los blogs de Liferay

Argitalpen data: 2019/05/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Liferay Portal 7.0 CE GA7 (7.0.6) eta zerbitzurik gabeko lehenagoko bertsioak.

Azalpena:

Christian Mehlmauer ikertzaileak ahultasun baten berri eman du, ataken eskaneatze erasoak egiteko erabil litezkeen blogetan *pingback* funtzionaltasunari eragiten diona.

Koponbidea:

- Ahultasun honetarako partxerik ez dago. Arintze neurri modura, pingback funtzionaltasuna desaktibatzea gomendatzen da. Ataria Liferay Portal 7.1 CE GA1 (7.1.0) edo geroagoko batera eguneratzea gomendatzen da.

Xehetasuna:

- Ahultasun hau baliatuz, urruneko erasotzaileek HTTP eskariak bidal ditzakete Interneteko zerbitzarietara, eta ataken eskaneatze erasoak egin ditzakete, jatorrizko URL faltsu bat zehaztuz.

Etiketak: Eguneraketa, Ahultasuna

Kodearen urruneko exekuzioa Citrix-en hainbat produktutan

Argitalpen data: 2019/05/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Windows-erako Receiver , LTSR 4.9 CU6 4.9.6001 baino lehenagoko bertsioak
- Citrix Workspace App, 1904 baino lehenagoko bertsioak

Azalpena:

NCC Group-eko Ollie Whitehouse, Richard Warren eta Martin Hill ikertzaileek kodearen urruneko exekuzio erako ahultasuna aurkitu dute Citrix-en Citrix Workspace App eta Windowserako Receiver produktuetan.

Koponbidea:

- Citrixek bezeroei gomendatzen die Citrix Workspace App-en 1904 edo geroagoko bertsiora eta Windows-erako Receiver-en LTSR 4.9 CU6 4.9.6001 bertsiora eguneratzea.

Xehetasuna:

- Ahultasun bat aurkitu da Citrix Workspace App eta Windowserako Receiver produktuetan, eta horren eraginez, unitate lokalerako sarbide hobespenak ez aplikatzea gerta liteke. Hori baliatuz, erasotzaile batek bezeroen unitate lokaletarako sarbidea irakur/idatz

lezake, eta horrela bezeroaren gailuan kodea urrunetik exekutatzea lor lezake. Ahultasun horretarako CVE-2019-11634 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Ahultasuna

Múltiples vulnerabilidades en productos Cisco

Argitalpen data: 2019/05/14

Garrantzia: Handia

Kaltetutako baliabideak:

- Cisco IOS XE softwarearen bertsio kaltetu bat erabiltzen duten Cisco gailuak, baldin eta HTTP zerbitzariaren funtzioa aktibatuta badute. HTTP Zerbitzaria funtzioaren egoera lehenetsia bertsioaren baitakoa da.
- Cisco Secure Boot hardwarearen aldaketa ahultasunak Ciscoren hainbat produkturi eragiten die, hardwarean oinarritutako abio seguruaren funtzionaltasuna onartzen dutenak. Zerrenda osoa ikusteko kaltetutako produktuen taula kontsultatu *Erreferentziak* atalean.

Azalpena:

Ciscok bi ahultasunen berri eman du. Horietako bat Cisco IOS XE Softwareren webean (Web UI) oinarritutako erabiltzaile interfazeak dauka, eta hori baliatuz autentifikatutako urruneko erasotzaile batek kaltetutako gailu baten azpiko shell Linux-ean komandoak exekuta litzake. Bestea Ciscoren Secure Boot-en dago, eta hori baliatuz osagaian firmwarearen irudi aldatu bat idatz liteke.

Konponbidea:

- Ciscok doako software eguneraketak argitaratu ditu, ohartarazpen honetan azaltzen diren ahultasunei erantzuten dietenak.

Xehetasuna:

- Kaltetutako softwareak modu okerrean garbitzen du Cisco IOS XE Softwareren webean (Web UI) oinarritutako erabiltzaile interfazean erabiltzaileak ematen duen sarrera. Kaltetutako gailura administratzaile sarbidea lukeen erasotzaile batek ahultasun hori balia lezake bereziki diseinatutako sarrera parametro bat emanez, formulario batean, Webaren erabiltzaile interfazean, eta ondoren hura bidaliz. Horri esker erasotzaileak komando arbitrarioak exekuta litzake gailuan root pribilegioekin, eta horren ondorioz sistema osorik jar liteke arriskuan. Ahultasun horretarako CVE-2019-1862 identifikatzailea esleitu da.
- *Field Programmable Gate Array-ren* (FPGA) abio seguruko hardwarearen inplementazioaren zati baten eguneraketak *in situ* kudeatzen dituen kodearen areak duen egiaztatzeko oker bat baliatuz, pribilegio altuak dituen eta kaltetutako gailuan exekutatzen ari den azpiko sistema eragilera sarbidea lukeen erasotzaile batek FPGAn aldatutako firmware irudi bat idatz lezake. Horrela gailua erabilezin geldituko litzateke (eta hardwarea ordezkatzea eskatuko luke), edo abio seguruko egiaztapen prozesua manipulatuko litzateke, eta ondorioz egoera batzuetan erasotzaileak asmo gaiztoko softwarearen irudi bat instalatu eta abiatu ahal izango luke. Ahultasun horretarako CVE-2019-1649 identifikatzailea esleitu da.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Man-in-the-middle erako ahultasuna Samba-n

Argitalpen data: 2019/05/14

Garrantzia: Handia

Kaltetutako baliabideak:

- Samba 4.0z geroztikako bertsio guztiak.
- Heimdal-en bertsio guztiak, 0.8z geroztik eta 7.5.0 barne, eta Heimdal-en bertsio horiek erabiliz sortzen den KDC (Key Distribution Center) bat bidaltzen duen edozein produktu ere.

Azalpena:

Barneratutako KDC Heimdal-en handler S4U2Self-en egiten den checksum-aren baliozkotzeak ez du hasieran konfirmatzen checksum-a deszifratuta egotea, eta horrela ahalbidetzen da eskatutako xede nagusia (bezeroa) ordeztea.

Konponbidea:

- Ahultasun honi buruzko partxeak argitaratu dira Sambaren deskarga zentroan. Horrez gain, Sambaren 4.8.12, 4.9.8 eta 4.10.3 bertsioak argitaratu dira, akatsa konpontzeko segurtasun partxe modura. Sambaren administratzaileei aholkatzen zaie bertsio horietara eguneratzea edo partxea lehenbailehen aplikatzea.

Xehetasuna:

- Akats bat dago Sambaren Active Directory (AD) Domain Controller-en (DC), Heimdalen KDCn. Eskatzen den segurtasun entitatea aldaketetatik babesteko Heimdal KDC-k S4U2Self paketean zerbitzariak kokatzen duen checksuma egiaztatzen duenean, ez du egiaztatzen eskarian erabiltzaile izena babesten duen checksum algoritmoa zifratuta ote dagoen. Egoera honek man-in-the-middle erako eraso bat egitea ahalbidetzen du. Horren bitartez eskaria atzeman eta alda daiteke, eskariaren erabiltzaile izena aldatuz eta KDCn dagoen beste edozein erabiltzaileren izenarekin ordeztuz. Ahultasun horretarako CVE-2018-16860 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Komunikazioak, Samba, Ahultasuna

Hainbat ahultasun Cisco produktuetan

Argitalpen data: 2019/05/16

Garantzia: Kritikoa

Kaltetutako baliabideak:

- Cisco PI Software, 3.4.1, 3.5 eta 3.6 baino lehenagoko bertsioak.
- EPN Manager, 3.0.1 baino lehenagoko bertsioak.
- Cisco Aggregation Services Router (ASR) 9000 Series, ondoko baldintzak betetzen direnean:
  - Routerra Cisco IOS XR Software exekutatzen ari denean, 5.3.3 Service Pack 10 bertsioa.
  - Routerrak MPLS OAM funtzionaltasuna konfiguratuta dauka.
- Cisco Webex Business Suite, WBS39.2.205 bertsioa baino lehenagoko Webex Network Recording Player eta Webex Player-en bertsio guztiak.
- Cisco Webex Meetings Online, 1.3.42 bertsioa baino lehenagoko Webex Network Recording Player eta Webex Player-en bertsio guztiak.
- Cisco Webex Meetings Server, 2.8MR3 SecurityPatch2, 3.0MR2 SecurityPatch2, edo 4.0 de Webex Network Recording Player baino lehenagoko bertsio guztiak.
- Small Business Sx200, Sx300, Sx500, ESW2 Series Managed Switches.
- Small Business Sx250, Sx350, Sx550 Series Switches.
- Firepower:
  - 4100 Series.
  - 9300 Security Appliances.
- MDS 9000 Series Multilayer Switches
- Nexus 1000V:
  - Para Microsoft Hyper-V.
  - Para VMware vSphere.
- Nexus Series Switches:
  - 3000.
  - 6000.
  - 7000.
  - 7700.
  - 9000 en modo *standalone* NX-OS.
- Nexus Platform Switches:
  - 3500.
  - 5500.
  - 5600.
- Nexus 9000 Series Fabric Switches en modo Application Centric Infrastructure (ACI).
- Nexus 9500 R-Series Switching Platform.
- Cisco IOS XR Software :
  - 32-bit.
  - 64-bit.
- Cisco Video Surveillance Manager, versión 7.12.0, si se está ejecutando en los modos Operations Manager, Media Server, Maps Server, o Federator.

Azalpena:

Ciscok 13 ahultasunen berri eman du, horietatik 3 kritikoak eta gainerakoak larritasun altukoak.

Konponbidea:

- Ciscok ahultasunak konpontzen dituzten eguneraketak argitaratu ditu, kaltetutako produktuaren arabera. Eguneraketak eskuragarri daude Ciscoren softwarearen deskarga panelean.

Xehetasuna:

- Larritasun kritikoko hiru ahultasunak baliatuz, urruneko erasotzaile batek azpiko sistema eragilean kode arbitrarioa exekutatzeko gaitasuna eskura lezake pribilegio altuekin. Horietatik lehena, CVE-2019-1821, autentifikatu gabeko erasotzaile baten aldetik baliatua izan liteke, baldin eta kaltetutako interfaze administratibora sare sarbidea badu. Bigarrenari eta hirugarrenari dagokienez, CVE-2019-1822 eta CVE-2019-1823, beharrezkoa da erasotzaileak kredentzial baliagarriak izatea kaltetutako interfaze administratiboan autentifikatzeko.
- Larritasun altuko gaineko ahultasunek ondorengo ekintzak eragin litzakete kaltetutako produktuetan:
  - Zerbitzuaren ukapena: CVE-2019-1846, CVE-2019-1806, CVE-2019-1858 eta CVE-2019-1849.
  - Kodearen exekuzio arbitrarioa: CVE-2019-1771, CVE-2019-1772 eta CVE-2019-1773.
  - SQL injekzioa: CVE-2019-1824 eta CVE-2019-1825.
  - Informazioa zabaltzea: CVE-2019-1717.

Etiketak: Eguneraketa, Cisco, Ahultasuna

Hainbat ahultasun Citrix Hypervisor-en

Argitalpen data: 2019/05/16

Garrantzia: Handia

Kaltetutako baliabideak:

- XenServer 7.6,
- XenServer 7.1 LTSR Cumulative Update 2,
- XenServer 7.0,
- Citrix Hypervisor 8.0.

Azalpena:

Citrix-ek CPU batzuen hardwareari eragiten dioten hainbat ahultasunen berri eman du:

Konponbidea:

- Citrix Hypervisor eguneratzea..
- CPUaren mikrokodea eguneratzea komando honen bidez: xl dmesg | grep *'Hardware features:*'
- CPUaren *hyper-threading* desgaitzea (aldibereko *multi-threading* modura ere ezaguna). Hori guztia egiteko urratsak ondoko dokumentuan jasotzen dira.

Gainera, gerta liteke sistema eragileen eguneraketak behar izatea bai eta *host* sistemaren *firmware*-arena (BIOS) ere, hornitzailearen

argibideak jarraiki.

Xehetasuna:

- CPUaren hardwareak dituen hainbat ahultasun baliatuz, CPUaren nukleo berean exekutatzen ari diren edo duela gutxi exekutatu diren beste prozesuenak, makina birtualenak edo hiperbisorearenak diren memoria datuen balioa ondorioztatu lezake CPUaren nukleoan pribilegiorik gabe exekutatzen den kodeak. Ahultasun horietarako CVE-2018-12126, CVE-2018-12127, CVE-2018-12130 eta CVE-2019-11091 identifikatzaileak erreserbatu dira.

Etiketak: Eguneraketa, Ahultasuna

DoS erako ahultasuna Liferay-n

Argitalpen data: 2019/05/16

Garrantzia: Handia

Kaltetutako baliabideak:

- Liferay Faces Alloy, Servlet (non-Portlet) 3.0 ingurunea.

Azalpena:

Liferay Faces Alloy-k erasotzaileei ahalbidetzen die fitxategi oso handiak igotzea, Servlet (ez Portlet) ingurune batean zerbitzuaren ukapen erako eraso batean erabil litekeena.

Konponbidea:

- Kaltetutako bertsioaren arabera partxe egokia aplikatzea, 2.0.2 edo 3.0.2.

Detalle:

- Ahultasun honek ez die eragiten Liferay Faces Alloy-k erabiltzen dituen *portlet*-ei (web atari batean kudeatzen eta bistaratzen diren erabiltzaile interfazeen osagai modularrak). Nolanahi ere, duela gutxi aurkitu eta zuzendutako ahultasun batek (DoS via large file upload), portlet ingurune batean *com.liferay.faces.util.uploadedFileMaxSize* baliozkotzea saihets dadin eragiten du.

Etiketak: Eguneraketa, Ahultasuna

Kodearen urruneko exekuzioa IBMren WebSphere Application Server-en

Argitalpen data: 2019/05/16

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- WebSphere Application Server ND, 9.0 bertsioa
- WebSphere Application Server ND, 8.5 bertsioa
- WebSphere Virtual Enterprise, 7.0 bertsioa

Azalpena:

IBMko Ryan Wincey-k WebSphere Application Server Network Deployment-ek duen kodearen urruneko exekuzio erako ahultasun baten berri eman du.

Konponbidea:

Gomendatutako konponbidea da ahalik azkarren behin-behineko partxea aplikatzea, produktu bakoitzerako APARa duen Fixpack edo PTF.

- WebSphere Application Server ND tradicional eta WebSphere Application Server ND Hypervisor Edition-en kasuan, 9.0.0.0tik 9.0.0.11ra bitarteko bertsioak:
  - fixpack-en gutxieneko mailetara eguneratzea, behin-behineko partxeak eskatzen duenaren arabera, eta ondoren PH11655 behin-behineko konponbidea aplikatzea, edo bestelao
  - fixpack 9.0.0.12 edo ondorenekoa aplikatzea (aurreikuspenen arabera, 2019ko bigarren hiruhilekoan eskuragarri).
- WebSphere Application Server ND tradicional eta WebSphere Application Server ND Hypervisor Edition-en kasuan, 8.5.0.0tik 8.5.5.15ra bitarteko bertsioak:
  - fixpack-en gutxieneko mailetara eguneratzea, behin-behineko partxeak eskatzen duenaren arabera, eta ondoren PH11655 behin-behineko konponbidea aplikatzea, edo bestela
  - fixpack 8.5.5.16 edo ondorenekoa aplikatzea (aurreikuspenen arabera, 2019ko hirugarren hiruhilekoan eskuragarri).
- WebSphere Virtual Enterprise Edition v7.0ren kasuan: PH11655 behin-behineko partxea aplikatzea.
  - OHARRA: WebSphere Virtual Enterprise V7 zerbitzuz kanpo dago. Horregatik, IBMk gomendatzen du produktua eguneratzea zerbitzua duen bertsio, release edo plataforma batera.

Xehetasuna:

- IBM WebSphere Application Server NDk ahalbidetu liezaioke urruneko erasotzaile bati sisteman kode arbitrarioa exekutatzea, fidagarriak ez diren iturrietatik serializatutako objektuen sekuentzia batekin, bereziki diseinatutakoa. Ahultasun horretarako CVE-2019-4279 kodea erreserbatu da.

Etiketak: IBM, Ahultasuna

DLLren bahiketa FortiClient-en

Argitalpen data: 2019/05/17

Garrantzia: Handia

Kaltetutako baliabideak:

- FortiClient for Windows, 6.0.6 bertsioa baino lehenagokoak.

Azalpena:

FortiClient-en online instalatzaileak duen bilaketa bide ez-seguru erako ahultasun baten berri eman da. Hori baliatuz autentifikatu gabeko urruneko erasotzaile batek kode arbitrarioa exekuta lezake sisteman.

Konponbidea:

- Windows-erako FortiClient 6.0.6 bertsiora edo ondoreneko batera eguneratzea.

Xehetasuna:

- FortiClient-en online instalatzaileak duen bilaketa bide ez-seguru erako ahultasun bat baliatuz, autentifikatu gabeko urruneko erasotzaile batek, FortiClientOnlineInstaller.exe dagoen direktorioaren kontrola balu, kode arbitrarioa exekuta lezake sisteman, direktorio horretan asmo gaiztoko dll fitxategiak kargatuz. Ahultasun horretarako CVE-2019-5589 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun HPEren Integrated Lights-Out 4 eta 5en

Argitalpen data: 2019/05/20

Garrantzia: Handia

Kaltetutako baliabideak:

- HPE Gen10 zerbitzarietarako HPE Integrated Lights-Out 5 (iLO 5), 1.39 eta lehenagoko bertsioak,
- HPE Integrated Lights-Out 4 (iLO 4), 2.61b eta lehenagoko bertsioak.

Azalpena:

HPk bere Integrated Lights-Out (iLO) produktuek dituzten hainbat ahultasunen berri eman du. Horiek baliatuz urruneko erasotzaile batek *Cross-Site Scripting* (XSS) egin lezake, baimenik gabeko datuak injektatu eta bufferraren gainezkatzea eragin.

Konponbidea:

- iLO 4ren kasuan, *firmware*-aren 2.70 bertsiora edo ondoreneko batera eguneratzea.
- iLO 5en kasuan, *firmware*-aren 1.40a bertsiora edo ondoreneko batera eguneratzea.

Xehetasuna:

- Gen9 zerbitzarietarako HPE Integrated Lights-Out 4-k (iLO 4) dituen ahultasunak eta Gen10 zerbitzarietarako HPE Integrated Lights-Out 5-ek (iLO 5) dituenak baliatuz, urruneko erasotzaile batek ondokoa egin lezake: Cross-Site Scripting (XSS) erasoak, baimenik gabeko datuen injekzioa eta bufferraren gainezkatzea. Ahultasun horietarako ondoko identifikatzaileak erreserbatu dira: CVE-2019-11982 eta CVE-2019-11983. Eta CVE-2018-7117 identifikatzailea esleitu da.

Etiketak: Eguneraketa, HP, Ahultasuna

Hainbat ahultasun Moodle-n

Argitalpen data: 2019/05/20

Garrantzia: Handia

Kaltetutako baliabideak:

- 3.6tik 3.6.3ra bitartekoak, 3.5etik 3.5.5era bitartekoak, 3.4tik 3.4.8ra bitartekoak, 3.1etik 3.1.17ra bitartekoak eta zerbitzurik gabeko lehenagoko bertsioak.

Azalpena:

Moodle plataforman 3 ahultasun aurkitu dira, bat kritikotasun altukoa eta beste bi kritikotasun baxukoak.

Konponbidea:

- 3.7, 3.6.4, 3.5.6, 3.4.9 eta 3.1.18 bertsioetara eguneratzea.

Xehetasuna:

- Mezularitza web zerbitzu batek erabiltzailearen elkarrizketetakoak ez diren mezuak berreskuratzen ditu, eta kritikotasun altuko ahultasuna baliatuz, erabiltzaileak elkarrizketa guztiak ikus litzake. Ahultasun horretarako CVE-2019-10132 identifikatzailea erreserbatu da.

Kritikotasun baxuko gainerako ahultasunetarako honako identifikatzaile hauek erreserbatu dira: CVE-2019-10133 eta CVE-2019-10134.

Etiketak: Eguneraketa, CMS, Ahultasuna

Pribilegioen eskalatzea IBM MQ-n

Argitalpen data: 2019/05/23

Garrantzia: Handia

Kaltetutako baliabideak:

- IBM MQ V8
  - 8.0.0.0 - 8.0.0.11 bertsioak
- IBM MQ V9 LTS
  - 9.0.0.0 - 9.0.0.5 bertsioak
- IBM MQ V9.1 LTS
  - 9.1.0.0 - 9.1.0.1 bertsioak
- IBM MQ V9.1 CD
  - 9.1.1 bertsioa

Azalpena:

Kritikotasun altuko ahultasun bat aurkitu da IBM MQ-n. Hori baliatuz erasotzaile batek kodea exekuta lezake administratzaile baimenekin.

Konponbidea:

Ondoko eguneraketak aplikatzea, IBM MQren kaltetutako bertsioaren arabera:

- IBM MQ V8, 8.0.0.12
- IBM MQ V9 LTS, 9.0.0.6
- IBM MQ V9.1 LTS, 9.1.0.2
- IBM MQ V9.1 CD, 9.1.2

Xehetasuna:

- Ahultasunaren arrazoia da IBM MQren instalazio direktorioek duten baimenen konfigurazio okerra. Pribilegiorik gabeko erasotzaile lokal batek kodea exekutatzea lor lezake administratzaile baimenekin. Ahultasun horretarako CVE-2019-4078 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, IBM, Ahultasuna

Path transbertsal erako ahultasuna Bitbucket Data Center-en

Argitalpen data: 2019/05/24

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Bitbucket Data Center, honako bertsioak:

- 6.1.0tik 6.1.1era bitartekoak
- 6.0.0tik 6.0.2ra bitartekoak
- 5.16.0tik 5.16.2ra bitartekoak
- 5.15.0tik 5.15.2ra bitartekoak
- 5.14.0tik 5.14.3ra bitartekoak
- 5.13.0tik 5.13.5era bitartekoak

Azalpena:

RIPS Technologies-eko Johannes Moritz-ek Bitbucket Data Center migrazio tresnan larritasun kritikoko ahultasun bat aurkitu du, *path transversal* erakoa (alegia, direktorioen bideen murrizpen okerra). Horrek kodearen urruneko exekuzioa ahalbidetu lezake Datuen Zentroko lizentzia duten bertsioetan.

Konponbidea:

Atlassian-ek gomendatzen du Bitbucket Data Center-en azken bertsiora eguneratzea. Horren azalpena bertsioaren oharretan ikus daiteke. Bitbucket Data Center-en azken bertsioa deskargen zentrotik jaits daiteke.

- Bitbucket Data Center 6.1.2 bertsiora edo goragoko batera eguneratzea.
- 6.1.2 bertsiora eguneratzerik ez badago, ahultasun hori konpontzeko partxeak dituzten ondoko bertsioetara eguneratu, deskargatzeko eskuragarri daudenak:
  - 6.0.x bertsioak exekutatzen ari bazara 6.0.3 bertsiora eguneratu
  - 5.16.x bertsioak exekutatzen ari bazara 5.16.3 bertsiora eguneratu
  - 5.15.x bertsioak exekutatzen ari bazara 5.15.3 bertsiora eguneratu
  - 5.14.x bertsioak exekutatzen ari bazara 5.14.4 bertsiora eguneratu
  - 5.13.x bertsioak exekutatzen ari bazara 5.13.6 bertsiora eguneratu

Xehetasuna:

- Administratzaile baimenak dituen erabiltzaile autentifikatua duen urruneko erasotzaile batek direktorioen bideen murrizpen okerreko ahultasun hau (path transversal) balia lezake fitxategiak idazteko kokapen arbitrarioetan. Horren ondorioz kodearen urruneko exekuzioa gerta liteke Bitbucket Data Center-en bertsio ahul bat exekutatzen duten sistemetan. Datuen Zentroko lizentziarik ez duten Bitbucket Server-en bertsioek ez daukate ahultasun hori. Ahultasun horretarako CVE-2019-3397 kodea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna

Hainbat ahultasun FortiGuard-en FortiOS-en

Argitalpen data: 2019/05/27

Garrantzia: Handia

Kaltetutako baliabideak:

FortiOS, honako bertsioak:

- 6.0.0tik 6.0.4ra bitartekoak
- 5.6.0tik 5.6.8ra bitartekoak
- 5.4.1etik 5.4.10era bitartekoak
- 5.4.0 eta beheragoko bertsioak (5.2 adarra barne) ez daude kaltetuta.

CVE-2018-13382 identifikatzailea duen ahultasunaren kasuan, produktua soilik dago kaltetua SSL VPN web ataria gaituta baldin badago.

Azalpena:

DEVCORE Security Research Team-eko Meh Chang eta Orange Tsai ikertzaileek direktorioko jauzi eta baimentze oker erako bi ahultasunen berri eman dute.

Konponbidea:

- FortiOSen 5.4.11, 5.6.9, 6.0.5, 6.2.0 edo goragoko bertsioetara eguneratzea.

Xehetasuna:

- FortiOS SSL VPN web atariak duen direktorioko jauzi erako ahultasun bat baliatuz, autentifikatu gabeko erasotzaile batek FortiOSeko sistemako fitxategiak deskarga litzake bereziki diseinatutako HTTP baliabideen eskarien bidez, eta horrela informazioaren hedapena eragingo luke. Ahultasun horretarako CVE-2018-13379 identifikatzailea erreserbatu da.
- SSL VPN web atariak duen baimentze okerreko ahultasun bat baliatuz, autentifikatu gabeko erasotzaile batek SSL VPN web atari bateko erabiltzaile baten pasahitza alda lezake bereziki diseinatutako HTTP eskarien bidez. Ahultasun horretarako CVE-2018-13382 identifikatzailea erreserbatu da.

Etiketak: Eguneraketa, Ahultasuna