2020ko Abuztuaren Bulletina

Ohartarazpenak - Teknikoak

Komandoen injekzioaren ahultasuna NETGEAR R8300 sisteman

Argitalpen data: 2020/08/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Router NETGEAR R8300, 1.0.2.134 bertsioaren aurreko *firmware* bertsioak.

Azalpena:

Ikertzaile independente batek larritasun kritikoko ahultasun baten berri eman dio NETGEAR erakundeari. NETGEAR R8300 routerrari eragiten dio.

Konponbidea:

Kaltetutako produktuaren azken firmware bertsioa deskargatzea.

Xehetasuna:

NETGEAR erakundeak segurtasun-ahultasun bat konpondu du, fabrikatzaileari SSD Secure Disclosure programaren bidez bidalia. R8300 router modeloaren egiaztatzearen aurreko komandoen injekzio motakoa da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna

2020ko abuztuko SAP segurtasunaren eguneratzea

Argitalpen data: 2020/08/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP NetWeaver (ABAP Server) y ABAP Platform, versiones 702, 730, 731, 740 y 750.
- SAP NetWeaver AS JAVA (LM Configuration Wizard), 7.30, 7.31, 7.40 eta 7.50 bertsioak;
- SAP NetWeaver (Knowledge Management), 7.30, 7.31, 7.40 eta 7.50 bertsioak;
- SAP Business Objects Business Intelligence Platform, 4.2 eta 4.3 bertsioak;
- SAP Banking Services (Generic Market Data), 400, 450 eta 500 bertsioak;
- SAP NetWeaver (ABAP Server) eta ABAP Platform, 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 753 eta 755 bertsioak;
- SAP NetWeaver AS JAVA (ENGINEAPI), 7.10 eta 7.10 bertsioak;
- SAP NetWeaver AS JAVA (WSRM), 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50 bertsioak;
- SAP NetWeaver AS JAVA (SERVERCORE), 7.10, 7.10 eta 7.11 bertsioak;
- SAP NetWeaver AS JAVA (J2EE-FRMW), J2EE-FRMW 7.10 eta 7.11 bertsioak;
- SAP NetWeaver (Knowledge Management), 7.30, 7.31, 7.40 eta 7.50 bertsioak;
- SAP Adaptive Server Enterprise, 16.0 bertsioa;
- SAP Commerce, 6.7, 1808, 1811, 1905 eta 2005 bertsioak;
- SAP Data Intelligence, 3 bertsioa;
- SAPUI5 (UISAPUI5_JAVA), 7.50 bertsioa;
- SAPUI5 (SAP_UI), 750, 751, 752, 753, 754 eta 755 bertsioak;

- SAPUI5 (UI_700), 200 bertsioa;
- SAP ERP (HCM Travel Management), 600, 602, 603, 604, 605, 606, 607 eta 608 bertsioa;
- SAP Business Objects Business Intelligence Platform (Central Management Console), 4.2 eta 4.3 bertsioak;
- SAP S/4 HANA (Fiori UI for General Ledger Accounting), 103 eta 104 bertsioak;
- SAP NetWeaver (ABAP Server) eta ABAP Platform, 740, 750, 751, 752, 753, 754 eta 755 bertsioak;
- SAP NetWeaver (ABAP Server) eta ABAP Platform, 702, 730, 731, 740 eta 750 bertsioak.

Azalpena:

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

Konponbidea:

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

Xehetasunak:

SAPek 15 segurtasun ohar eta eguneratze 1 egin ditu bere hileroko jakinarazpenean. Horietako 2 larritasun kritikokoak dira, 6 altukoak eta 8 tartekoak.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Kodearen injekzioaren ahultasun bat.
- *Cross-site scripting* motako 5 ahultasun.
- Informazioaren dibulgazioaren arloko 4 ahultasun,
- Baimenaren konprobatze faltaren 3 ahultasun,
- Egiaztatzea konprobatze faltaren 4 ahultasun,
- Beste motaren bateko ahultasun bat.

Segurtasun ohar nabarmenenak honakoen ingurukoak dira:

- SAP NetWeaver AS JAVA (LM Configuration Wizard) sistemak ez du autentikazioa egiaztatzen. Horren bidez, aurretik egiaztatu gabeko erasotzaile batek konfigurazioak egin litzake SAP Java sistemaren aurkako ekintza kritikoak burutzeko, baita erabiltzaile administraria sortzeko gaitasuna ere, beraz, sistemaren eskuragarritasuna, integritatea eta konfidentzialtasuna konprometituta egon daitezke. Ahultasun horretarako, CVE-2020-6287 identifikatzailea esleitu da.

- SAP Enterprise Portal-en SAP NetWeaver sistemaren parte den SAP Knowledge Management delakoari eragiten dion Cross-Site Scripting (XSS) motako ahultasun bat. Horren bidez, sistemaren eskuragarritasuna, konfidentzialtasuna eta integritatea konprometituta egon daitezke. Ahultasun horretarako, CVE-2020-6284 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2020-6294, CVE-2020-6298, CVE-2020-6296, CVE-2020-6309, CVE-2020-6293, CVE-2020-6295, CVE-2020-6297, CVE-2020-6301, CVE-2020-6300, CVE-2020-6273, CVE-2020-6299 eta CVE-2020-6310.

Etiketak: Eguneratzea, SAP, Ahultasuna

Microsoften segurtasun buletina. 2020ko abuztua

Argitalpen data: 2020/08/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based)
- Microsoft ChakraCore
- Internet Explorer
- Microsoft Scripting Engine
- SQL Server
- Microsoft JET Database Engine
- .NET Framework
- ASP.NET Core
- Microsoft Office and Microsoft Office Services and Web Apps
- Microsoft Windows Codecs Library
- Microsoft Dynamics

Azalpena:

Segurtasun eguneratzeen inguruko abuztuko Microsoft argitalpenean 124 ahultasun jaso dira oraingoan; 14 kritiko gisa sailkatu dira eta 103 garrantzitsu gisa.

Konponbidea:

Dagokion segurtasun-eguneratzea instalatzea. Microsoften orrian eguneratze horiek egiteko azalpenak eman dira.

Xehetasunak:

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Pribilegioak handitzea,
- Zerbitzua ukatzea.
- Kodearen urrutiko exekuzioa.
- Informazioa zabaltzea.

- Nortasuna ordeztea (spoofing).

GARRANTZITSUA: Microsoftek adierazi du bi ahultasun aktiboki baliatzen ari direla erasotzaileak, zehazki Internet Explorer 11 sistemari eragiten dion urrutiko exekuzio arloko ahultasun bat; CVE-2020-1380 identifikatzailea esleitu zaio. Beste ahultasunak Windowsen hainbat produkturi eragiten die, eta nortasuna ordezteko balio dezake; CVE-2020-1464 identifikatzailea esleitu zaio.

Etiketak: Eguneratzea, Microsoft, Nabigatzailea, Ahultasuna, Windows.

Hainbat ahultasun Intel Server Boards, Server Systems eta Compute Modules sistemetan

Argitalpen data: 2020/08/12

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Intel Server System R1000WT, R2000WT, R1000SP, LSVRP, LR1304SP, R1000WF eta R2000WF,
- Intel Server Boards S2600WT, S2600CW, S2600KP, S2600TP, S1200SP, S2600WF, S2600ST eta S2600BP,
- Intel Compute Module HNS2600KP, HNS2600TP eta HNS2600BP.

Azalpena:

Intelek Intel Server System, Server Boards eta Compute Module sistemen hainbat ahultasunen berri eman du. Horien bidez, erasotzaile batek pribilegioetan gora egin lezake, edo zerbitzu ukapena eragin.

Konponbidea:

Intelek firmware bertsio berri bat argitaratu du kaltetutako produktuentzat. Zerrenda zehatza kontsulta daiteke web orrian.

Xehetasunak:

Guztira 22 ahultasun aurkitu dira; horietako 1 kritikoa eta 10 garrantzia handikoak.

Ahultasunik kritikoena 1.59 bertsioaren aurreko Intel Server Boards, Server Systems eta Compute Modules sistemen plaka batzuen egiaztatze-sistemen akats bati dagokio. Horren bidez, egiaztatu gabeko erasotzaile batek pribilegioetan gora egin lezake, ondoko sarbide baten bidez. Ahultasun horretarako, CVE-2020-8708 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Pribatutasuna, Ahultasuna

Hainbat ahultasun Citrix Endpoint Management sisteman (CEM)

Argitalpen data: 2020/08/13

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- XenMobile Server 10.12, RP3ren aurreko bertsioak,
- XenMobile Server 10.11, RP6ren aurreko bertsioak,
- XenMobile Server 10.10, RP6ren aurreko bertsioak,
- XenMobile Server 10.9, RP5aren aurreko bertsioak.

Azalpena:

Positive Technologies, Tradecraft eta Detectify erakundeetako ikertzaileek Citrix Endpoint Management (CEM) sistemari eragiten dioten hainbat ahultasunen berri eman dute (XenMobile gisa ere ezaguna da). Ahultasun horien bidez, egiaztatu gabeko erasotzaile batek administrari pribilegioak lortu litzake gailuan.

Konponbidea:

Citrix etxeak honako bertsioetarako partxeak argitaratu ditu:

- XenMobile Server 10.12 RP3,
- XenMobile Server 10.11 RP6,
- XenMobile Server 10.10 RP6,
- XenMobile Server 10.9 RP5.

Xehetasunak:

Citrix erakundeak ez du atzemandako ahultasunei buruzko xehetasun teknikorik partekatu, baina Positive Technologies enpresak jakinarazi du ahultasunetako bat qutxienez ibilbide-jauzi bati (Path Traversal) dagokiola. Horren bidez, erasotzaile batek artxibo arbitrarioak irakur litzake web zerbitzariaren jatorrizko direktoriotik kanpo, datu konfidentzialetarako zifratze gakoak eta konfigurazio artxiboak barne. Kritikotzat jotako ahultasun horretarako, CVE-2020-8209 identifikatzailea erreserbatu da.

Ahultasun hauetarako erreserbatutako beste identifikatzaile batzuk honakoak dira: CVE-2020-8208, kritikotzat jo dena, eta

CVE-2020-8210, CVE-2020-8211 eta CVE-2020-8212, nolabaiteko kritikotasun maila eta maila baxuarekin.

Etiketak: Eguneratzea, Komunikazioak, Birtualizazioa, Ahultasuna

---

Hainbat ahultasun Apache Struts 2 sisteman

Argitalpen data: 2020/08/17

Garrantzia: Handia

Kaltetutako baliabideak:

Apache Struts 2, 2.0.0 eta 2.5.20 bitarteko bertsioak.

Azalpena:

Apple Information Security erakundeko Matthias Kaiser eta Mitsui Bussan Secure Directions Inc. Enpresako Takeshi Terada ikertzaileek larritasun handi eta ertaineko 2 ahultasunen berri eman dute; kodearen urrutiko exekuzio eta zerbitzuaren ukapenari dagozkio, hurrenez hurren.

Konponbidea:

Apache Struts 2 sistema 2.5.22 bertsiora eguneratzea.

Xehetasunak:

- Apache Struts sistemako *framework* delakoek, konprobatzea bortxatzen denean, etiketa-atributu jakin batzuei (hala nola id) esleitutako atributuen balioen ebaluazio bikoitza egiten dute, beraz, posible izango litzateke etiketa baten atributuak erakusten direnean berriz ere ebaluatuko den balio bat pasatzea. Arazo hori aplikatzen da soilik OGNL ebaluazioa Struts etiketaren atributu baten barruan sendotzen denean, ebaluatzeko adierazpenak balioztatu eta prozesatu gabeko sarrera bati erreferentzia egiten dionean, erasotzaile batek zuzenean aldatu lezakeena, dagokion eskaera sortuz eta kodearen urrutiko exekuzio-egoera posible bat sortuz (RCE). Ahultasun horretarako CVE-2019-0230 kodea erreserbatu da

Tarteko larritasuna duen ahultasunerako CVE-2019-0233 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Apache, Ahultasuna

Jenkins sistemaren core elementuari eragiten dioten ahultasunak

Argitalpen data: 2020/08/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Jenkins 2.251 bertsiora arte, hori barne.
- Jenkins LTS 2.235.4 bertsiora arte, hori barne.

Azalpena:

Hainbat ikertzailek eman dute Jenkins sistemaren core elementuari eragiten dioten ahultasun batzuen berri. Zehazki, bat larritasun kritikokoa da, eta 3 larritasun altukoak. Motak: bufferraren ustelkeria eta biltegiratutako *Cross-Site Scripting* (XSS), hurrenez hurren.

Konponbidea:

Honako ahultasunak konpontzeko bertsio hauek instalatzea gomendatzen da:

- Jenkins, 2.252 bertsioa.
- Jenkins LTS, 2.235.5 bertsioa.

Xehetasuna:

- Jenkins softwareak *Winstone-Jetty* dauka barne, *Jetty wrapper* bat, http eta *servlet* moduan jarduteko. Horrek ahultasun bat dauka, eta, horren ondorioz, baimendu gabeko erasotzaileek HTTP erantzun goiburuak lor litzakete, beste erabiltzaile bati bideratutako datu konfidentzialekin. Ahultasun horretarako, CVE-2019-17638 identifikatzailea esleitu da.
- Jenkinsek ez ditu ondo sanitizatzen laguntza ikonoen tresnen gaineko informazio edukia, artikuluaren sorkuntzan erakusten den proiektuaren izenaren estrategiaren deskribapena, ezta *Trigger builds remotely* sistemaren bidez konpilazioa hasten duen host-aren urrutiko helbidea ere. Horren ondorioz, XSS motako ahultasunak sortu litezke. Ahultasun horietarako CVE-2020-2229, CVE-2020-2230 eta CVE-2020-2231 identifikatzaileak esleitu dira.

Era berean, Jenkins etxeak jakinarazi du beste osagarri batzuetan ere ahultasunak badaudela.

Etiketak: Eguneratzea, Ahultasuna

Hainbat ahultasun HPE etxearen HP-UX CIFS sisteman

Argitalpen data: 2020/08/19

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HP-UX Common Internet File System (CIFS) Client/Server Software, B.04.09.00.00 bertsioa eta aurrekoak

Azalpena:

HPE produktuen segurtasun taldeak 4 ahultasunen berri eman du. Horietako bat larritasun kritikokoa da, eta besteak ertainekoak. Motak: Direktorio mugatu baterako ibilbidearen izenaren mugatze desegokia (*path traversal*) eta mugetatik kanpoko irakurketa.

Konponbidea:

HP-UX CIFS Client/Server Software eguneratzea B.04.12.03.00 bertsiora.

Xehetasuna:

- Erasotzaile batek, tokikoa zein urrunekoa, ahultasun kritikoa baliatu lezake direktorio partekatu bati ihes egin eta baimendu gabeko informazioa lortzeko. Ahultasun horretarako, CVE-2019-10197 identifikatzailea esleitu da.

Gainerako ahultasunetarako, identifikatzaile batzuk esleitu dira: CVE-2019-10218, CVE-2019-14907 eta CVE-2019-3880.

Etiketak: Eguneratzea, HP, Ahultasuna

Ciscoren produktu batzuetan berezko kredentzialak erabiltzea

Argitalpen data: 2020/08/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Ahultasun honek Cisco ENCS 5400-W eta CSP 5000-W serieetako gailuei eragiten die Cisco vWAAS exekutatzen badute (6.4.5 edo 6.4.3d bertsioak eta NFVIS irudi paketatuak dituzten aurrekoak).

Azalpena:

Ahultasun hori barneko segurtasun-probetan atzeman zen. Kritikoa da, berezko kredentzialak eta estatikoak erabiltzen dituztenen motakoa.

Konponbidea:

Ciscok ahultasun hori konpondu zuen Cisco vWAAS sisteman, 6.4.3e, 6.4.5a bertsioekin eta NFVIS irudi paketatuaren osteko bertsioekin. Ciscoren deskarga zentroan eskuragarri daude.

OHARRA: ENCS 5400-W eta CSP 5000-W serieko gailuek ez dute aurreko bertsioetako vWAAS 6.4.3e eta 6.4.5a bertsioetarako eguneratzerik onartzen. Dagoeneko zuzenduta dagoen bertsio bat exekutatzeko, bezeroek instalazio berri bat egin behar dute ENCS 5400-W eta CSP 5000-W gailuetarako, Cisco WAAS pakete bateratuaren bertsioarekin.

Xehetasuna:

Baimenik gabeko urrutiko erasotzaile bat kaltetutako produktu baten NFVIS (*NFV Infrastructure Software*) sistemaren CLI (Command Line Interface) interfazera sar liteke, berezko kredentzialak dituzten kontuak erabiliz. Horrela, administrari pribilegioak lortu litzakete. Ahultasun horretarako, CVE-2020-3446 identifikatzailea erreserbatu da.

Etiketak: Eguneratzea, Cisco, Ahultasuna

Hainbat ahultasun Xen, Hypervisor eta XenServer sistemetan

Argitalpen data: 2020/08/25

Garrantzia: Handia

Kaltetutako baliabideak:

- Xen bertsio guztiak;
- Citrix Hypervisor 8.2 LTSR;
- Citrix Hypervisor 8.1;

- Citrix Hypervisor 8.0;
- Citrix XenServer 7.1 LTSR CU2;
- Citrix XenServer 7.0.

Azalpena:

QEMUri eragiten dioten hainbat ahultasunen berri eman da. Horien ondorioz, erasotzaile batek kodea exekuta lezake VM gonbidatu batean, QEMU prozesuaren host pribilegioekin, edo zerbitzuan ukapen bat egin (DoS).

Konponbidea:

Honako bertsioak instalatzea gomendatzen da:

- Xen-erako eskuragarri dago partxea;
- Citrix Hypervisor 8.2 LTSR: CTX280214;
- Citrix Hypervisor 8.1: CTX280213;
- Citrix Hypervisor 8.0: CTX280212;
- Citrix XenServer 7.1 LTSR CU2: CTX280211;
- Citrix XenServer 7.0: CTX280210.

Xehetasuna:

Citrix Hypervisor eta Xen sistemei eragiten dieten ahultasunak identifikatu dira QEMU delakoan. Horien bidez, QEMUren USB emuladorean mugetatik kanpoko irakurketa/idazketarako sarbidea baimendu liteke, eta konfigurazio batzuetan VM gonbidatu batean kode pribilegiatua exekutatu, *host* funtzioa potentzialki konprometituz.

Argitaratutako ahultasunek honako identifikatzaileak dituzte esleituta: CVE-2018-17958 eta CVE-2020-14364.

Etiketak: Eguneratzea, Birtualizazioa, Ahultasuna