2020ko Abenduaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun HPE produktu batzuetan

Argitalpen data: 2020/12/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- HP-UX Perl Software E.5.28.0.A;
- HPE Edgeline Infrastructure Management Software, 1.21 bertsioaren aurrekoak.

Azalpena:

Larritasun kritikoko hainbat ahultasunen bidez, erasotzaile batek bufferrak gainez egitea edo kode arbitrarioa exekutatzea eragin dezake.

Konponbidea:

Eguneratzea:

- Perl E.5.28.0.B;
- HPE Edgeline Infrastructure Manager, 1.21 bertsioa edo goragokoa.

Xehetasunak:

- Ahultasun batzuen ondorioz, erasotzaile batek bufferrak gainezka egitea eragin lezake, bereziki diseinatutako ohiko espresioen, idazketa operazio ez baliodunen bidez, gaizki eratutako bytecode intrusio-injekzioen bidez edota memoriaren heap eremuko buffer-gainezkatzeen bidez. Ahultasun horietarako CVE-2018-18311, CVE-2018-18312, CVE-2020-10543, CVE-2020-10878 eta CVE-2020-12723identifikatzaileak esleitu dira.
- HPE Edgeline Infrastructure Manager ahultasuna, HPE Edgeline Infrastructure Management Software gisa ere ezaguna, urrunetik erabil liteke benetako baimena saihesteko, eta erasotzaile batek komandoak exekutatu litzake sarbide pribilegiatua lortzeko, zerbitzuaren ukapena egiteko edo konfigurazioa aldatzeko. Ahultasun horretarako, CVE-2020-7199 identifikatzailea esleitu da.

Etiketak: Eguneratzea, HP, Ahultasuna

Hainbat ahultasun HPE sisteman

Argitalpen data: 2020/12/02

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HP-UX Web Server Suite Software ? HP-UX Apache-based Web Server, 2.4.18.05 bertsioa eta aurrekoak.

Azalpena:

Hewlett Packard Enterprise erakundeak honakoak identifikatu ditu: larritasun kritikoko 2 ahultasun, larritasun handiko 8 ahultasun, eta tarteko larritasuna duten 5 ahultasun. Denak dira urrutiko exekuziokoak, eta larritasun kritikoa dutenen bidez, erasotzaile batek informazio sentikorra zabaldu eta kodea exekuta lezake.

Konponbidea:

Eguneratzea:

- HP-UX Web Server Suite, bertsio honetara: 5.10;
- HP-UX Apache-based Web Server, bertsio honetara: 2.4.43.01.

Xehetasunak:

HPE HP-UX Web Server Suiteko bi ahultasunen bidez, Apache HP-UX 11iv3 sisteman exekutatuz, erasotzaile batek urrutiko kodea exekuta lezake, edo datu sentikorrak zabaldu. Ahultasun horietarako CVE-2019-10082 eta CVE-2020-11984 identifikatzaileak erreserbatu dira.

Larritasun kritikoko ahultasunei honako identifikatzaileak esleitu zaizkie: CVE-2018-8011, CVE-2019-0190, CVE-2019-0215, CVE-2019-10081, CVE-2019-10097, CVE-2019-9517, CVE-2020-11993 eta CVE-2020-9490.

Larritasun handiko ahultasunei honakoak esleitu zaizkie: CVE-2019-10092, CVE-2019-10098, CVE-2020-11985, CVE-2020-1927 eta CVE-2020-1934.

Etiketak: Eguneratzea, Apache, HP, Ahultasuna.

Hainbat ahultasun HPEren HP-UX Web Server Suite Software PHP sisteman

Argitalpen data: 2020/12/04

Garrantzia: Crítica

Kaltetutako baliabideak:

HP-UX Web Server Suite Software PHP, 7.2.1.1 bertsioa.

Azalpena:

Hewlett Packard Enterprise eta HPE Product Security Response Team taldeek 13 ahultasun antzeman dituzte guztira. 2 larritasun kritikokoak dira, 5 handikoak eta 6 tartekoak. Horren ondorioz, tokiko zein urrutiko erasotzaile batek segurtasun mugaketak gainditu litzake, informazioa zabaldu eta memoriaren korrupzioa burutu.

Konponbidea:

Produktua bertsio honetara eguneratzea: PHP 7.4.7.1, HP-UX Release B.11.31rako.

Xehetasunak:

- Fgetss() funtzioa erabiltzen denean datuak etiketa-garbiketarekin irakurtzeko (stripping tags), hainbat PHP bertsiotan posible izango litzateke esleitutako bufferretik harago irakurtzeko aukera ematen duten datuak ematea. Horren ondorioz, informazioa erakusgai jarri edo blokeo bat gerta liteke. Ahultasun kritiko horretarako, CVE-2020-7059 identifikatzailea esleitu da.
- Multibyte kodifikazioak eraldatzeko mbstring funtzioak erabiltzen direnean, hainbat PHP bertsiotan posible izango litzateke mbfl_filt_conv_big5_wchar funtzioak esleitutako bufferretik harago irakurtzeko aukera ematea. Horren ondorioz, informazioa erakusgai jarri edo blokeo bat gerta liteke. Ahultasun kritiko horretarako, CVE-2020-7060 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak esleitu dira: CVE-2020-7067, CVE-2019-11048, CVE-2020-7066, CVE-2020-7064, CVE-2019-11046, CVE-2019-11044, CVE-2019-11045, CVE-2019-11050, CVE-2019-11047, CVE-2019-11042 eta CVE-2019-11041.

Etiketak: Eguneratzea, HP, PHP, Ahultasuna

Microsoften segurtasun-eguneratzeak. 2020ko abendua.

Argitalpen data: 2020/12/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows;
- Microsoft Edge (EdgeHTML sistemas oinarritua);
- Microsoft Edge para Android;
- ChakraCore;
- Microsoft Office, Microsoft Office Services eta Web Apps;
- Microsoft Exchange Server;
- Azure DevOps;
- Microsoft Dynamics;
- Visual Studio;
- Azure SDK;
- Azure Sphere.

Azalpena:

Segurtasun eguneratzeen inguruko abenduko Microsoft argitalpenean 58 ahultasun jaso dira, eta abisu bat (ADV200013); 9 kritiko gisa sailkatu dira, 48 garrantzitsu gisa eta 2 moderatu gisa.

Konponbidea:

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

Xehetasunak:

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Pribilegioak handitzea,
- Informazioa zabaltzea.
- Kodearen urrutiko exekuzioa.
- Segurtasun-neurriak saihestea,
- Nortasuna ordeztea (spoofing).

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

2020ko abenduko SAP segurtasunaren eguneratzea

Argitalpen data: 2020/12/09

Garrantzia: Kritikoa

Kaltetutako baliabideak

- SAP NetWeaver AS JAVA, bertsioak: 7.10, 7.11, 7.20, 7.30, 7.31, 7.40 eta 7.50;
- SAP NetWeaver AS ABAP, bertsioak: 620, 640, 700, 710, 730, 731, 740, 750, 751, 752, 753 eta 754;
- SAP BusinessObjects BI Platform (Crystal Report), bertsioak: 4.1, 4.2 eta 4.3;
- SAP Business Warehouse, bertsioak: 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755 eta 782;
- SAP BW4HANA, bertsioak: 100 eta 200;
- SAP S4 HANA, bertsioak: 101, 102, 103, 104 eta 105;
- SAP Solution Manager, 7.20 bertsioa;
- SAP Disclosure Management, 10.1 bertsioa;
- SAP UI, bertsioak: 7.5, 7.51, 7.52, 7.53 eta 7.54;
- SAP UI 700, 2.0 bertsioa;
- SAP HANA Database, 2.0 bertsioa.

Azalpena

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

Konponbidea:

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

Xehetasunak:

SAPek, segurtasun-partxeen hileroko komunikazioan, 11 segurtasun ohar eta eguneratze 2 egin ditu. Horietako 3 larritasun kritikokoak dira, 2 altukoak, 5 tartekoak eta 1 baxukoa.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- Kodearen injekzioaren 2 ahultasun,
- Baimenaren konprobatze faltaren 2 ahultasun,
- Cross-site Scripting motako (XSS) ahultasun bat,
- Direktorio mugatu baterako sarbidearen mugatze desegokiaren motako ahultasun bat (path traversal),
- Baimen faltaren arloko ahultasun bat;
- XML balioztatze faltaren ahultasun bat,
- Beste motaren bateko 6 ahultasun.

Segurtasun ohar nabarmenenak honakoen ingurukoak dira:

- Ahultasun horren bidez, TCP portuetara konektatzeko gai den baimenik gabeko erasotzaile batek hainbat ekintza pribilegiatu egin litzake, hala nola konfiantzazko SSO hornitzaile berriak instalatzea, datu-basearen konexio-parametroak aldatzea eta konfigurazio-informaziorako sarbidea lortzea. Ahultasun horretarako, CVE-2020-26829 identifikatzailea esleitu da.
- Oinarrizko pribilegioak dituen erasotzaile batek XML entitate arbitrarioak injektatu litzake, eta horien bidez barne artxibo eta direktorioak zabalduko lirateke, SSRF eta DoS motako erasoak baimenduz. Ahultasun horretarako, CVE-2020-26831 identifikatzailea esleitu da.
- Pribilegio handiko erasotzaile batek bereziki landutako eskaerak bidal litzake, kode arbitrarioa sortu eta exekutatzeko, erabiltzailearen bestelako interakziorik gabe, eta, beraz, sistemaren konfidentzialtasuna, integritatea eta eskuragarritasuna konprometituta geratuko lirateke. Ahultasun horretarako, CVE-2020-26838 identifikatzailea esleitu da.
- Ahultasun horren bidez, urrutiko erasotzaile batek kode arbitrarioa injektatu eta exekutatu lezake, eta, horrela, kaltetutako sistemaren kontrol osoa eskuratuko luke. Ahultasun horretarako, CVE-2020-26808 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2020-26837, CVE-2020-26830, CVE-2020-26832, CVE-2020-26826, CVE-2020-26828, CVE-2020-26816, CVE-2020-26835, CVE-2019-0388, CVE-2020-26834 eta CVE-2020-26836.

Etiketak: Eguneratzea, SAP, Ahultasuna

Hainbat ahultasun ArubaOS sisteman

Argitalpen data: 2020/12/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Kaltetutako bertsioak honakoak dira:

- ArubaOS: 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0, eta aurrekoak.
- SD-WAN: 2.1.0.1, 2.2.0.0, eta aurrekoak.

Bertsio horiek honako produktuetan erabiltzen dira:

- ArubaOS Mobility Conductor.
- Aruba Mobility Controllers.
- Mobility Controller tresnek kudeatutako Access-Point.
- Aruba SD-WAN Gateways.

Azalpena:

Arubak ArubaOS-erako partxeak argitaratu ditu. Hainbat segurtasun-ahultasun hartzen dituzte barne, horietako bi oso kritikoak dira, eta erasotzaile batek urrutiko kodearen exekuzioa burutu lezake, edo komando arbitrarioen injekzioa.

Konponbidea:

ArubaOS honako bertsioetara eguneratzea gomendatzen dute:

- ArubaOS 6.4.4.24, 6.5.4.18, 8.2.2.10, 8.3.0.14, 8.5.0.11, 8.6.0.6, 8.7.1.0, eta hurrengoak.
- SD-WAN 2.1.0.2, 2.2.0.1, eta hurrengoak.

Xehetasuna:

Arubak zuzendutako ahultasunak honako ahultasun kritikoen bidez konpontzen dira:

- Tarteko memoriaren gainezkatze arloko ahultasuna. Kodearen exekuzioa gerta liteke, bereziki landutako paketeak PAPIk erabilitako (Aruba Networks AP management protocol) UDP (8211) portura bidaliz. Ahultasun horretarako, CVE-2020-24633 identifikatzailea esleitu da.
- Komando arbitrarioen urrutiko injekzioaren ahultasuna, bereziki landutako paketeak PAPIk erabilitako (Aruba Networks AP management protocol) UDP (8211) portura bidaliz. Ahultasun horretarako, CVE-2020-24634 identifikatzailea esleitu da.

Honako identifikatzaileak dituzten ahultasunerako partxeak ere argitaratu dira: CVE-2020-10713 eta CVE-2020-24637.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Kredentzial barneratuen ahultasuna IBM Spectrum Protect Plus sisteman

Argitalpen data: 2020/12/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

IBM Spectrum Protect Plus, 10.1.0etik 10.1.6ra bitarteko bertsioak.

Azalpena:

Tenablek larritasun kritikoko ahultasun bat antzeman du, kredentzial barneratuen motakoa.

Konponbidea:

10.1.7 bertsiora eguneratzea.

Xehetasuna:

Kaltetutako produktuak modu estatikoan kodifikatutako kredentzialak ditu, eta bere sarbidea, irteera komunikazioak eta barne-datuen zifratzea baimentzeko erabiltzen ditu. Horrela, erasotzaile batek pribilegio handiak lortu litzake urrunetik. Ahultasun horretarako, CVE-2020-4854 identifikatzailea esleitu da.

Etiketak: Eguneratzea, IBM, Ahultasuna.

Kodearen urrutiko exekuzioaren ahultasuna Apache Struts sisteman

Argitalpen data: 2020/12/09

Garrantzia: Handia

Kaltetutako baliabideak:

Struts, 2.0.0 eta 2.5.25 bertsioen bitartekoak.

Azalpena:

GitHub erakundeko Álvaro Muñoz eta Aeye Security Lab-eko Masato Anzai ikertzaileek larritasun handiko ahultasun baten berri eman dute. Kodearen urrutiko exekuzioaren motakoa da.

Konponbidea:

OGNL (Object Graph Navigation Language) ebaluazio bortxatua saihestea eta bertsioa edo goragokoa eguneratzea.

Xehetasuna:

Konfiantzazkoa ez den erabiltzaile baten sarrera-balioen OGNL ebaluazio bortxatuaren ondorioz, kodearen urrutiko exekuzioa gerta liteke (RCE). Ahultasun horretarako, CVE-2020-17530 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Apache, Java, Ahultasuna.

Hainbat ahultasun Cisco Jabber sisteman

Argitalpen data: 2020/12/11

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Windowserako Cisco Jabber, bertsioak:
  - 12.1 aurrekoak;
  - 12.1;
  - 12.5;
  - 12.6;
  - 12.7;
  - 12.8;
  - 12.9.
- MacOS-erako Cisco Jabber, bertsioak:
  - 12.7 eta aurrekoak;
  - 12.8;
  - 12.9.
- Android eta iOS-erako Cisco Jabber, bertsioak:
  - 12.8 eta aurrekoak;
  - 12.9.

Azalpena:

Olav Sortland Thoresen, Watchcom erakundeko ikertzaileak, segurtasun-proba batzuk burutu zituen Cisco-ko talde batekin batera, 5 ahultasun antzeman ditu: 1 larritasun kritikokoa, 2 larritasun handikoak eta beste 2 tartekoak. Motak: bidalitako datuetan informazio sentikorra sartzea, komandoen injekzioa, sistema eragilearen komandoen injekzioa, informazioa zabaltzea eta kodearen exekuzio arbitrarioa.

Konponbidea:

- Windowserako Cisco Jabber, bertsioak:
  - 12.1.4;
  - 12.5.3
  - 12.6.4;
  - 12.7.3;
  - 12.8.4;
  - 12.9.3.
- MacOS-erako Cisco Jabber, bertsioak:
  - 12.8.5;
  - 12.9.4.
- Android eta iOS-erako Cisco Jabber, 12.9.4 bertsioa:

Xehetasuna:

- Ahultasun kritikoa mezuen edukiaren balioztatze desegokiari zor zaio. Baimena lortu duen urrutiko erasotzaile batek ahultasun hori baliatu lezake kaltetutako produktuei bereziki diseinatutako XMPP mezuak bidaltzeko, kode arbitrarioaren exekuzioan eraginez. Ahultasun horretarako, CVE-2020-26085 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak esleitu dira: CVE-2020-27134, CVE-2020-27133, CVE-2020-27132 eta CVE-2020-27127.

Etiketak: Eguneratzea, Cisco, Komunikazioak, Ahultasuna.

SolarWinds Orion Platform tresnaren aurkako esplotazio kanpaina aktiboa

Argitalpen data: 2020/12/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

SolarWinds Orion Platform, 2019.4 HF 5 bertsiotik 2020.2.1era artekoak, 2020ko martxoa eta 2020ko ekaina bitartean argitaratuak.

Azalpena:

FireEye etxeak intrusio kanpaina global bat antzeman du, eta horren erantzuleen atzetik dabil, UNC2452, esaterako. SolarWinds Orion Platform eguneratzea gomendatzen da, 2020.2.1 HF 1 bertsiora, ahalik eta arinen; izan ere, ahultasun hori modu aktiboan baliatu daiteke.

Konponbidea:

SolarWinds Orion Platform ahalik eta arinen eguneratzea gomendatzen da, 2020.2.1 HF 1 bertsiora. Hemen dago eskuragarri: SolarWinds Customer Portal. Ahultasun hori aktiboki baliatu liteke. Berehala eguneratu ezin bada, mesedez, egin kasu jarraibideei, hemen, SolarWinds Orion Platform-eko instantzia ziurtatzeko.

Ez badakizu ziur zein Orion Platform bertsio erabiltzen ari zaren, kontsultatu jarraibideak hemen. Zein hotfix aplikatu duzun jakiteko, kontsultatu hemen.

Aurreikusi da 2020ko abenduaren 15ean hotfix-en bertsio berri bat argitaratuko dela, 2020.2.1 HF 2. Bezero guztiei gomendatzen zaie bertsio horretara eguneratzea, izan ere, 2020.2.1 HF 2 bertsioak ordeztu egiten du konprometituta dagoen osagaia, eta segurtasun-hobekuntza gehiago dakartza.

Xehetasuna:

FireEye etxeak antzeman du hornikuntza-katean eraso bat egon dela, SolarWinds Orion enpresa-softwarearen eguneratzeak troianizatu ditu, SUNBURST izeneko *backdoor* motako malware bat zabaltzeko. Kanpaina oso hedatuta dago eta mundu osoko erakunde pribatu eta publikoei eragiten die. Erantzuleak UNC2452 izenez ezagutzen dira.

Malwareak OIP (*Orion Improvement Program*) protokolo moduan maskaratzen du sare-trafikoa, eta errekonozimenduaren emaitzak legezko *pluginen* konfigurazio artxiboetan biltegiratzen ditu, beraz, SolarWinds-en legezko jardueran ezkuta daiteke. *Backdoor* delakoak hainbat blokeo-zerrenda itsu erabiltzen ditu prozesu, zerbitzu eta kontrolatzaile gisa exekutatzen diren antibirusak eta bestelako tresnak identifikatzeko.

Horniketa-katearen konpromiso horren osteko jardueraren barruan alboko mugimendua eta datuen lapurreta egon dira. FireEye erakundea mehatxu hori antzemateko sinadurak argitaratzen ari da.

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

Hainbat ahultasun ABB produktu batzuetan

Argitalpen data: 2020/12/16

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- ABB Ability™ Symphony®Plus:
  - S Operations 1.1;
  - S Operations 2.0, Service Packs guztiak;
  - S Operations 2.1, Service Pack 1 (SP1), Melody eta bestelako Heritage sistemetarako;
  - S Operations 2.1, Service Pack 2 (SP2);
  - S Operations 3.0;
  - S Operations 3.1;
  - S Operations 3.2;
  - S Operations 3.3.
- ABB Ability™ Symphony®Plus:
  - S Historian 3.0 eta 3.1.
- ABB Central Licensing System (CLS) hemen: ABB AbilityTM Symphony Plus Operations (3.0 eta 3.3 bitartean);
- ABB Central Licensing System (CLS) hemen: ABB AbilityTM Symphony Plus Engineering (1.0 eta 2.3 bitartean);
- ABB Central Licensing System (CLS) hemen: Composer Harmony (5.1, 6.0 eta 6.1);
- ABB Central Licensing System (CLS) hemen: Composer Melody (5.3 eta 6.1);
- ABB Central Licensing System (CLS) hemen: HarmonyOPC Server (6.0, 6.1 eta 7.0);

Azalpena:

ABB erakundeak hainbat ahultasunen berri eman du. Horien bidez, erasotzaile batek kaltetutako produktuen funtzionalitateez abusatu lezake.

Konponbidea:

- S Operations-erako:
  - 3.3 Service Pack 1 bertsiora eguneratzea
- S Operations-erako, 3.X bertsioaren aurrekoak, hiru eguneratze hauek aurreikusten dira:
  - Q4 2020: S Operations 2.1 SP 2 Rollup 2 (Harmony, SD eta Freelance);
  - Q1 2021: S Operations 2.2 (Melody eta Procontrol P14);
  - Q3 2021: S Operations 2.2 Rollup 1 (Procontrol P13).
- Para ABB Ability^{TM} Symphony®Plus:
  - S Historian 3.2 bertsiora eguneratzea.
- Sym-phony Plus, Composer Harmony, Composer Melody eta HarmonyOPC Server-erako:
  - Eskuragarri dagoen azken bertsiora eguneratzea eta 2PAA121231 oharrean azaldutako segurtasun-neurri orokorrak aplikatzea.

Xehetasuna:

- ABB AbilityTM Symphony®Plus Operations eta ABB AbilityTM Symphony®Plus Historian produktuei eragiten dieten ahultasun motak:
  - .SQL Injection. Ahultasun horretarako, CVE-2020-24673 identifikatzailea esleitu da.
  - Egiaztatze-metodo ahula. Ahultasun horretarako, CVE-2020-24675 identifikatzailea esleitu da.
  - Egiaztatzerik eza. S Operations sistemari soilik eragiten dio. Ahultasun horretarako, CVE-2020-24683 identifikatzailea esleitu da.
- Sym-phony Plus, Composer Harmony, Composer Melody eta HarmonyOPC Server produktuei eragiten dieten ahultasun motak:
  - XXE. Ahultasun horretarako, CVE-2020-8479 identifikatzailea esleitu da.
  - Informazioa zabaltzea. Ahultasun horretarako, CVE-2020-8481 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2020-24674, CVE-2020-24676, CVE-2020-24677, CVE-2020-24678, CVE-2020-24679, CVE-2020-24680, CVE-2020-8481 eta CVE-2020-8471.

Etiketak: Eguneratzea, Ahultasuna

Kodearen urrutiko exekuzioaren motako ahultasuna HPE Systems Insight Manager (SIM) sisteman

Argitalpen data: 2020/12/16

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HPE Systems Insight Manager (SIM), 7.6.x bertsioak.

Azalpena:

Harrison Neal ikertzaileak, Trend Micro Zero Day Initiative ekimenaren bidez, Hewlett Packard Enterprise erakundeari jakinarazi dio ahultasun bat antzeman duela, eta, horren bidez, HPE Systems Insight Manager (SIM) sisteman urrutiko exekuzioa burutu litekeela.

Konponbidea:

HPE etxeak jakinarazi du etorkizunean bertsio bat argitaratuko duela ahultasun hori konpontzeko, eta "Federated Search" eta "Federated CMS Configuration" funtzioak ezabatzeko honako urratsak jarraitzea gomendatu du:

1. HPE SIM zerbitzua gelditzea.
2. Honako artxiboa ezabatzea, *< C:Program FilesHPSystems Insight Managerjbossserverhpsimdeploysimsearch.war > instalazio-ibilbidetik: /Q /F C:Program FilesHPSystems Insight Managerjbossserverhpsimdeploysimsearch.war.*
3. HPE SIM zerbitzua berrabiaraztea.
4. HPE SIM-en https://SIM_IP:50000 webgunera sartu ahal izan arte itxaron, eta sistemaren sinbolotik komando hau exekutatu*: mxtool -r -f toolsmulti-cms-search.xml 1 >nul 2 >nul.*

Xehetasuna:

Ahultasun bat antzeman da HPE Systems Insight Manager (SIM) sisteman, 7.6. bertsioa. Ahultasun horren bidez, kodearen urrutiko exekuzioa burutu liteke. Ahultasun horretarako, CVE-2020-7200 identifikatzailea esleitu da.

Etiketak: HP, Ahultasuna

Hainbat ahultasun Netgear produktuetan

Argitalpen data: 2020/12/17

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- DGN2200v1, v1.0.0.60 bertsioaren aurreko *firmware* bertsioak;
-
- SXK80, 3.1.0.104 bertsioaren aurreko *firmware* bertsioak;

- NMS300, 1.6.0.27 bertsioaren aurreko *firmware* bertsioak.

Azalpena:

Netgear etxeak bere produktuei eragiten dieten larritasun kritikoko hainbat ahultasun argitaratu ditu.

Konponbidea:

Netgear-en laguntza orrira sartu eta kaltetutako gailuaren azken firmware bertsioa deskargatzea.

Xehetasuna:

Ahultasun motak honakoak dira:

- HTTPd egiaztatze motako ahultasuna.
-
- Funtzio-mailako sarbide-kontrolik eza.
- Egiaztatu aurreko komando-injekzioa.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Kodearen urrutiko exekuzioaren ahultasuna HPE iLO Amplifier Pack sisteman

Argitalpen data: 2020/12/18

Garrantzia: Kritikoa

Kaltetutako baliabideak:

iLO Amplifier Pack, 1.70 bertsioa.

Azalpena:

Erik de Jong ikertzaileak Hewlett Packard Enterprise erakundeari jakinarazi dio larritasun kritikoko ahultasun bat antzeman duela. Mota: kodearen urrutiko exekuzioa.

Konponbidea:

1.71 bertsiora eguneratzea.

Xehetasuna:

HPE iLO Amplifier Pack zerbitzariko segurtasun-ahultasun baten ondorioz, erasotzaile batek kodearen urrutiko exekuzioa burutu lezake (RCE). Ahultasun horretarako, CVE-2020-7203 identifikatzailea esleitu da.

Etiketak: Eguneratzea, HP, Ahultasuna

Netgear erakundearen Wi-Fi sistema eta router komandoen injekzioa

Argitalpen data: 2020/12/23

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- R6400v2, 1.0.4.84 bertsioaren aurreko firmware bertsioekin.
-
- R6700v3, 1.0.4.84 bertsioaren aurreko firmware bertsioekin.
- R6900P, 1.3.2.124 bertsioaren aurreko firmware bertsioekin.
- R7000, 1.0.11.100 bertsioaren aurreko firmware bertsioekin.
- R7000P, 1.3.2.124 bertsioaren aurreko firmware bertsioekin.
- R7800, 1.0.2.74 bertsioaren aurreko firmware bertsioekin.
- R7850, 1.0.5.60 bertsioaren aurreko firmware bertsioekin.
- R7900, 1.0.4.26 bertsioaren aurreko firmware bertsioekin.
- R7960P, 1.4.1.50 bertsioaren aurreko firmware bertsioekin.
- R8000, 1.0.4.52 bertsioaren aurreko firmware bertsioekin.
- R7900P, 1.4.1.50 bertsioaren aurreko firmware bertsioekin.
- R8000P, 1.4.1.50 bertsioaren aurreko firmware bertsioekin.
- RAX15, 1.0.1.64 bertsioaren aurreko firmware bertsioekin.
- RAX20, 1.0.1.64 bertsioaren aurreko firmware bertsioekin.
- RAX200, 1.0.1.12 bertsioaren aurreko firmware bertsioekin.
- RAX45, 1.0.2.66 bertsioaren aurreko firmware bertsioekin.
- RAX50, 1.0.2.66 bertsioaren aurreko firmware bertsioekin.
- RAX75, 1.0.3.102 bertsioaren aurreko firmware bertsioekin.
- RAX80, 1.0.3.102 bertsioaren aurreko firmware bertsioekin.
- RBK752, 3.2.16.6 bertsioaren aurreko firmware bertsioekin.
- RBR750, 3.2.16.6 bertsioaren aurreko firmware bertsioekin.

- RBS750, 3.2.16.6 bertsioaren aurreko firmware bertsioekin.
- RBK852, 3.2.15.25 bertsioaren aurreko firmware bertsioekin.
- RBR850, 3.2.15.25 bertsioaren aurreko firmware bertsioekin.
- RBS850, 3.2.15.25 bertsioaren aurreko firmware bertsioekin.
- RBK842, 3.2.15.25 bertsioaren aurreko firmware bertsioekin.
- RBR840, 3.2.15.25 bertsioaren aurreko firmware bertsioekin.
- RBS840, 3.2.15.25 bertsioaren aurreko firmware bertsioekin.
- RS400, 1.5.0.48 bertsioaren aurreko firmware bertsioekin.
- XR300, 1.0.3.50 bertsioaren aurreko firmware bertsioekin.

Azalpena:

Netgear erakundeak hainbat produkturi eragiten dien larritasun kritikoko ahultasun baten berri eman du. *Talsonor* ikertzaileak antzeman du.

Konponbidea: .

Netgear laguntza orrira sartu eta kaltetutako gailuen azken firmware bertsioa deskargatzea.

Xehetasuna:

Netgear etxeak zuzenketa batzuk argitaratu ditu, egiaztatzearen aurreko komandoen injekzio motako segurtasun-ahultasun baten harira.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Hainbat ahultasun Dell Wyse ThinOS sisteman

Argitalpen data: 2020/12/23

Garrantzia: Kritikoa

Kaltetutako baliabideak:

8.6 MR8 bertsioaren aurrekoak, bezeroak protokolo ez seguru baten bidez artxibo zerbitzari batetik konfigurazioak jasotzen dituen kasuetan, honako produktuetan:

- Dell Wyse 3040 Thin Client (ENG),
- Dell Wyse 3040 Thin Client (JPN),
- Dell Wyse 3040 Thin Client con PCoIP (ENG),
- Dell Wyse 3040 Thin Client con PCoIP (JPN),
- Dell Wyse 5010 Thin Client (ENG),
- Dell Wyse 5010 Thin Client (JPN),
- Dell Wyse 5010 Thin Client con PCoIP (ENG),
- Dell Wyse 5010 Thin Client con PCoIP (JPN),
- Dell Wyse 5040 Thin Client (ENG),
- Dell Wyse 5040 Thin Client (JPN),
- Dell Wyse 5040 Thin Client con PCoIP (ENG),
- Dell Wyse 5040 Thin Client con PCoIP (JPN),
- Dell Wyse 5060 Thin Client (ENG),
- Dell Wyse 5060 Thin Client (JPN),
- Dell Wyse 5060 Thin Client con PCoIP (ENG),
- Dell Wyse 5060 Thin Client con PCoIP (JPN),
- Dell Wyse 5070 Thin Client (ENG),
- Dell Wyse 5070 Thin Client (JPN),
- Dell Wyse 5070 Thin Client con PCoIP (ENG),
- Dell Wyse 5070 Thin Client con PCoIP (JPN),
- Dell Wyse 5470 AIO Thin Client (ENG),
- Dell Wyse 5470 AIO Thin Client (JPN),
- Dell Wyse 5470 AIO Thin Client con PCoIP (ENG),
- Dell Wyse 5470 AIO Thin Client con PCoIP (JPN),
- Dell Wyse 5470 Thin Client (ENG),
- Dell Wyse 5470 Thin Client (JPN),
- Dell Wyse 5470 Thin Client con PCoIP (ENG),
- Dell Wyse 5470 Thin Client con PCoIP (JPN),
- Dell Wyse 7010 Thin Client (ENG),
- Dell Wyse 7010 thin client (JPN).

Azalpena:

Bi ahultasunen berri eman da; biak larritasun kritikokoak, aldez aurretiko konfigurazioari dagokionez. Horien bidez, erasotzaile bat idazketa artxibo batera sar liteke, bezero zehatz baten konfigurazioa manipulatu eta informazio sentikorra eskuratu.

Konponbidea:

Honako bertsioetara eguneratzea:

- Dell Wyse 3040 Thin Client (ENG),
- Dell Wyse 3040 Thin Client (JPN),
- Dell Wyse 3040 Thin Client PCoIP (ENG),
- Dell Wyse 3040 Thin Client PCoIP (JPN),
- Dell Wyse 5010 Thin Client (ENG),
- Dell Wyse 5010 Thin Client (JPN),
- Dell Wyse 5010 Thin Client PCoIP (ENG),

- Dell Wyse 5010 Thin Client PCoIP (JPN),
- Dell Wyse 5040 Thin Client (ENG),
- Dell Wyse 5040 Thin Client (JPN),
- Dell Wyse 5040 Thin Client PCoIP (ENG),
- Dell Wyse 5040 Thin Client PCoIP (JPN),
- Dell Wyse 5060 Thin Client (ENG),
- Dell Wyse 5060 Thin Client (JPN),
- Dell Wyse 5060 Thin Client PCoIP (ENG),
- Dell Wyse 5060 Thin Client PCoIP (JPN),
- Dell Wyse 5070 Thin Client (ENG),
- Dell Wyse 5070 Thin Client (JPN),
- Dell Wyse 5070 Thin Client PCoIP (ENG),
- Dell Wyse 5070 Thin Client PCoIP (JPN),
- Dell Wyse 5470 AIO Thin Client (ENG),
- Dell Wyse 5470 AIO Thin Client (JPN),
- Dell Wyse 5470 AIO Thin Client PCoIP (ENG),
- Dell Wyse 5470 AIO Thin Client PCoIP (JPN),
- Dell Wyse 5470 Thin Client (ENG),
- Dell Wyse 5470 Thin Client (JPN),
- Dell Wyse 5470 Thin Client PCoIP (ENG),
- Dell Wyse 5470 Thin Client PCoIP (JPN),
- Dell Wyse 7010 Thin Client (ENG),
- Dell Wyse 7010 thin client (JPN).

Xehetasuna:

- Aldez aurretik zehaztutako konfigurazio ez seguruaren motako ahultasun baten ondorioz, urrutiko erasotzaile batek, baimenik gabe, tokiko sareko informazio sentikorra eskuratu lezake, eta horren ondorioz kaltetutako bezeroen konpromisoa gerta liteke. Ahultasun horretarako, CVE-2020-29491 identifikatzailea esleitu da.
- Aldez aurretiko konfigurazio ez seguruaren motako ahultasun baten ondorioz, urrutiko erasotzaile batek, baimenik gabe, idazketa-artxiborako sarbidea lortu lezake, eta xedeko edozein estazio espezifikoren konfigurazioa manipulatu. Ahultasun horretarako, CVE-2020-29492 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Komandoen urrutiko exekuzioa SolarWinds Orion erakundearen APIan

Argitalpen data: 2020/12/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Hauen aurreko bertsio guztiak:

- 2019.4 HF 6 (2020ko abenduaren 14an argitaratua);
- 2020.2.1 HF 2 (2020ko abenduaren 15ean argitaratua);
- 2019.2 SUPERNOVA Patch (2020ko abenduaren 23an argitaratua);
- 2018.4 SUPERNOVA Patch (2020ko abenduaren 23an argitaratua);
- 2018.2 SUPERNOVA Patch (2020ko abenduaren 23an argitaratua);

Azalpena:

Ahultasun bat antzeman da SolarWinds Orion plataforman. Horren bidez, produktuan barne dagoen APIaren egiaztatzea saihestu egin daiteke, beraz, erasotzaile batek komandoen urrutiko exekuzioa burutu lezake. Ahultasun hori SUPERNOVA izenez ezaguna den malwareak erabili du.

Hau aurretik identifikatutako beste segurtasun-arazoaren desberdina da. Izan ere, arazo hura SolarWinds Orionen aurkako esplotazio-kanpainaren baitan kokatzen da, hornidura -katearen bidez antzeman zen eta SUNBURST ezaguna erabiltzen zuen backdoor gisa.

Konponbidea:

Honako bertsioetara eguneratzea gomendatzen dute:

- 2019.4 HF 6 (2020ko abenduaren 14an argitaratua);
- 2020.2.1 HF 2 (2020ko abenduaren 15ean argitaratua);
- 2019.2 SUPERNOVA Patch (2020ko abenduaren 23an argitaratua);
- 2018.4 SUPERNOVA Patch (2020ko abenduaren 23an argitaratua);
- 2018.2 SUPERNOVA Patch (2020ko abenduaren 23an argitaratua);

Xehetasuna:

Ahultasun bat antzeman da. Horren bidez, SolarWinds Orion plataforman barne hartutako APIaren egiaztatzea saihestu daiteke. Request.PathInfo, eremuaren barruan URI eskaera batean parametro espezifikoak sartzean sortzen da ahultasuna. Horrela, erasotzaile batek baimenik gabeko API komandoak exekuta litzake, SolarWinds Orion zerbitzaritik *SkipAuthorization* flag delakoa lortuta. Ahultasun horretarako CVE-2020-10148 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Hainbat ahultasun Netgear produktu batzuetan

Argitalpen data: 2020/12/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- AC2100, 1.2.0.72 bertsioaren aurreko firmware bertsioak exekutatuz;
- AC2400, 1.2.0.72 bertsioaren aurreko firmware bertsioak exekutatuz;
- AC2600, 1.2.0.72 bertsioaren aurreko firmware bertsioak exekutatuz;
- CBK40, 2.5.0.10 bertsioaren aurreko firmware bertsioak exekutatuz;
- CBR40, 2.5.0.10 bertsioaren aurreko firmware bertsioak exekutatuz;
- D6000, 1.0.0.80 bertsioaren aurreko firmware bertsioak exekutatuz;
- D6220, 1.0.0.60 bertsioaren aurreko firmware bertsioak exekutatuz;
- D6400, 1.0.0.94 bertsioaren aurreko firmware bertsioak exekutatuz;
- D7000v2, 1.0.0.62 bertsioaren aurreko firmware bertsioak exekutatuz;
- D7800, 1.0.3.48 bertsioaren aurreko firmware bertsioak exekutatuz;
- D8500, 1.0.3.50 bertsioaren aurreko firmware bertsioak exekutatuz;
- DC112A, 1.0.0.48 bertsioaren aurreko firmware bertsioak exekutatuz;
- DGN2200v4, 1.0.0.114 bertsioaren aurreko firmware bertsioak exekutatuz;
- DM200, 1.0.0.66 bertsioaren aurreko firmware bertsioak exekutatuz;
- EAX20, 1.0.0.36 bertsioaren aurreko firmware bertsioak exekutatuz;
- EAX80, 1.0.1.62 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX2700, 1.0.1.58 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX3110, 1.0.1.68 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX3700, 1.0.0.84 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX3800, 1.0.0.84 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX3920, 1.0.0.84 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6000, 1.0.0.44 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6100v2, 1.0.1.94 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6110, 1.0.1.68 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6120, 1.0.0.54 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6130, 1.0.0.36 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6150v1, 1.0.0.46 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6150v2, 1.0.1.94 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6200v1, 1.0.3.94 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6250, 1.0.0.128 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6400, 1.0.2.152 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6400v2, 1.0.0.128 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6410, 1.0.0.128 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6920, 1.0.0.54 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX7000, 1.0.1.90 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX7300, 1.0.2.152 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX7300v2, 1.0.0.128 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX7320, 1.0.0.128 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX7500, 1.0.0.68 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX7700, 1.0.0.210 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX8000, 1.0.1.224 bertsioaren aurreko firmware bertsioak exekutatuz;
- MK62, 1.0.5.102 bertsioaren aurreko firmware bertsioak exekutatuz;
- MR60, 1.0.5.102 bertsioaren aurreko firmware bertsioak exekutatuz;
- MS60, 1.0.5.102 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6120, 1.0.0.70 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6220, 1.1.0.100 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6230, 1.1.0.100 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6250, 1.0.4.42 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6260, 1.1.0.76 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6300v2, 1.0.4.42 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6330, 1.1.0.76 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6350, 1.1.0.76 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6400v1, 1.0.1.62 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6400v2, 1.0.4.98 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6700v1, 1.0.2.16 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6700v2, 1.2.0.72 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6700v3, 1.0.4.98 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6800, 1.2.0.72 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6850, 1.1.0.76 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6900, 1.0.2.16 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6900P, 1.3.2.124 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7000, 1.0.11.106 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7000P, 1.3.2.124 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7100LG, 1.0.0.56 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7500v2, 1.0.3.48 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7800, 1.0.2.74 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7850, 1.0.5.60 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7900, 1.0.4.26 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7900P, 1.4.1.62 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7960P, 1.4.1.62 bertsioaren aurreko firmware bertsioak exekutatuz;
- R8000, 1.0.4.58 bertsioaren aurreko firmware bertsioak exekutatuz;
- R8000P, 1.4.1.62 bertsioaren aurreko firmware bertsioak exekutatuz;
- R8300, 1.0.2.134 bertsioaren aurreko firmware bertsioak exekutatuz;
- R8500, 1.0.2.134 bertsioaren aurreko firmware bertsioak exekutatuz;
- R8900, 1.0.5.24 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX120, 1.0.1.136 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX15, 1.0.1.64 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX20, 1.0.1.64 bertsioaren aurreko firmware bertsioak exekutatuz;

- RAX200, 1.0.5.24 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX35, 1.0.3.80 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX40, 1.0.3.80 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX45, 1.0.2.64 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX50, 1.0.2.64 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX75, 1.0.3.102 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX80, 1.0.3.102 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBK12, 2.6.1.44 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBR10, 2.6.1.44 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBS10, 2.6.1.44 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBK20, 2.6.1.38 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBR20, 2.6.1.36 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBS20, 2.6.1.38 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBK40, 2.6.1.38 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBR40, 2.6.1.38 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBS40, 2.6.1.38 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBK50, 2.6.1.40 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBR50, 2.6.1.40 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBS50, 2.6.1.40 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBR840, 3.2.16.6 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBS840, 3.2.16.6 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBR850, 3.2.16.6 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBS850, 3.2.16.6 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBS40V, 2.5.1.6 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBS40V-200, 1.0.0.46 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBS50Y, 2.6.1.40 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBW30, 2.5.0.4 bertsioaren aurreko firmware bertsioak exekutatuz;
- RS400, 1.5.0.48 bertsioaren aurreko firmware bertsioak exekutatuz;
- WN2500RPv2, 1.0.1.56 bertsioaren aurreko firmware bertsioak exekutatuz;
- WN3000RPv3, 1.0.2.86 bertsioaren aurreko firmware bertsioak exekutatuz;
- WN3500RPv1, 1.0.0.28 bertsioaren aurreko firmware bertsioak exekutatuz;
- WNDR3400v3, 1.0.1.32 bertsioaren aurreko firmware bertsioak exekutatuz;
- WNR1000v3, 1.0.2.78 bertsioaren aurreko firmware bertsioak exekutatuz;
- WNR2000v2, 1.2.0.12 bertsioaren aurreko firmware bertsioak exekutatuz;
- XR300, 1.0.3.50 bertsioaren aurreko firmware bertsioak exekutatuz;
- XR450, 2.3.2.66 bertsioaren aurreko firmware bertsioak exekutatuz;
- XR500, 2.3.2.66 bertsioaren aurreko firmware bertsioak exekutatuz;
- XR700, 1.0.1.34 bertsioaren aurreko firmware bertsioak exekutatuz;
- D7800, 1.0.1.58 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6400, 1.0.1.62 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6700, 1.0.2.16 bertsioaren aurreko firmware bertsioak exekutatuz;
- R6900v2, 1.2.0.72 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7200, 1.2.0.72 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7350, 1.2.0.72 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7400, 1.2.0.72 bertsioaren aurreko firmware bertsioak exekutatuz;
- R7450, 1.2.0.72 bertsioaren aurreko firmware bertsioak exekutatuz;
- R9000, 1.0.5.24 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX200, 1.0.2.102 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBK752, 3.2.16.6 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBR750, 3.2.16.6 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBS750, 3.2.16.6 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBK842, 3.2.16.6 bertsioaren aurreko firmware bertsioak exekutatuz;
- RBK852, 3.2.16.6 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6100, 1.0.2.28 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6150, 1.0.0.46 bertsioaren aurreko firmware bertsioak exekutatuz;
- EX6200, 1.0.3.94 bertsioaren aurreko firmware bertsioak exekutatuz;
- MK62, 1.0.4.98 bertsioaren aurreko firmware bertsioak exekutatuz;
- MR60, 1.0.4.98 bertsioaren aurreko firmware bertsioak exekutatuz;
- MS60, 1.0.4.98 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX45, 1.0.2.32 bertsioaren aurreko firmware bertsioak exekutatuz;
- RAX50, 1.0.2.32 bertsioaren aurreko firmware bertsioak exekutatuz;
- WN3500RP, 1.0.0.28 bertsioaren aurreko firmware bertsioak exekutatuz;
- WNR3500Lv2, 1.2.0.62 bertsioaren aurreko firmware bertsioak exekutatuz;
- XR300, 1.0.3.50 bertsioaren aurreko firmware bertsioak exekutatuz;

Azalpena:

Netgear erakundeak larritasun kritikoko hiru ahultasunen berri eman du. Florian Hehenberger eta Simon Birngruber ikertzaileek eman dute horiek berri, Austria Altuko Zientzia Aplikatuen Unibertsitatekoa, talsonor, eta SSD Secure Disclosure erakundekoa.

Konponbidea:

Netgear laguntza orrira sartu eta kaltetutako gailuen azken firmware bertsioa deskargatzea.

Xehetasuna:

Netgear etxeak hainbat eguneratze argitaratu ditu akatsak zuzentzeko: segurtasun konfigurazio akastunak, egiaztatu aurreko buffer gainezkatzeak eta egiaztatu aurreko komandoen injekzioa.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

batzuetan

Argitalpen data: 2020/12/28

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Backup Exec, bertsioak: BE 20.x, BE 21.x eta 16.x. Sostengurik ez duten aurreko bertsioak ere kaltetuta egon daitezke.
- Veritas System Recovery (VSR), Windowserako bertsioak soilik: 21.1, 21, 18.0.4, 18.0.3, 18.0.2, 18.0.1, 18.0, 16.0.2, 16.0.1 y 16. Sostengurik ez duten aurrekoak ere kaltetu daitezke.
- NetBackup y OpsCenter, 8.3.0.1 bertsioa eta aurrekoak. Windows plataformari soilik eragiten dio.
- VRP/NetBackup Resiliency Platform, 3.4 eta 3.5 bertsioak. Sostengurik ez duten aurreko bertsioak ere kaltetuta egon daitezke.
- Veritas InfoScale, Windowserako bertsioak: 7.4.2, 7.4.1, 7.4, 7.3.1, 7.3, 7.2, 7.1, 7.0.1 y 7.0; Storage Foundation HA, Windows 6.1rako; eta Storage Foundation, Windows 6.1rako. Sostengurik ez duten aurreko bertsioak ere kaltetu daitezke.
- Veritas InfoScale Operations Manager (VIOM), Windows Management Server-erako bertsioak: 7.4.2, 7.4, 7.3.1, 7.3, 7.2, 7.1 eta 7.0. Sostengurik ez duten aurreko bertsioak ere kaltetu daitezke.
- Enterprise Vault, bertsioak: 14.0, 12.5.2, 12.5.1, 12.5. 12.4.2. 12.4.1. 12.4, 12.3.2, 12.3.1, 12.3, 12.2.3, 12.2.2, 12.2.1, 12.2, 12.1.3, 12.1.2, 12.1.1, 12.1, 12.0.4, 12.0.3, 12.0.2, 12.0.1 y 12.0. Sostengurik ez duten aurreko bertsioak ere kaltetu daitezke.
- Veritas Desktop and Laptop Option (DLO), bertsioak: 9.3.3, 9.3.2, 9.3.1, 9.3, 9.2, 9.1, 9.0.1, 9.0 eta 9.5en aurrekoak. Sostengurik ez duten aurreko bertsioak ere kaltetu daitezke.
- NetBackup con CloudPoint, 8.3.0.1 eta 8.3 bertsioak.
- CloudPoint, bertsioak: 2.2.2, 2.2.1, 2.2, 2.1.2, 2.1.1, 2.1, 2.0.2, 2.0.1, 2.0, 1.0.2 eta 1.0.
- APTARE IT Analytics, bertsioak: 10.5 eta 10.4.

Azalpena:

Veritas erakundeak hainbat ohar argitaratu ditu. 11 ahultasun dira guztira, 10 kritikoak eta 1 tarteko larritasunekoa. Kritiko guztiak OpenSSL liburutegiarekin erlazionatuta daude.

Konponbidea:

Eguneratze hauek aplikatzea:

- Backup Exec 21.1 Hotfix 657517 (21.0.1200.1217 bertsioa);
- Backup Exec 20.6 Hotfix 298543 (20.0.1188.2734 bertsioa);
- Backup Exec 16.X bertsiorako eta aurrekoetarako: Fabrikatzailearen eguneratze-gomendioa: Backup Exec 21.2 bertsiora,
- Veritas System Recovery (VSR) 21.2;
- OpenSSL Hotfix para NetBackup 8.1.2, NetBackup 8.2, NetBackup 8.3 edo NetBackup 8.3.0.1;
- VRP/NetBackup Resiliency Platform v3.6 (2021eko urtarrilean eskuragarri) v3.4 edo v3.5erako partxea aplikatzea;
- Veritas Desktop and Laptop Option (DLO) 9.5 bertsioa;
- NetBackup 8.3.0.1 eta NetBackup-erako HotFix aplikatzea, CloudPoint osagaiekin batera.

Hotfix horiek eskuragarri daude Veritasen deskarga-gunean, deskargatu eta automatikoki instalatzeko.

Backup Exec produkturako konponbide alternatibo moduan, posible da administrari kontu baten bidez 'usrlocalssl' direktorioa sortzea, unitate guztien sustraiaren mende, eta direktorioaren ACL ezartzea, gainerako erabiltzaileei idazketa sarbidea ukatzeko. Horrela, erasotzaile batek OpenSSL motor maltzur bat instalatzea saihestuko da.

Xehetasuna:

Windows sisteman pribilegio gutxi dituen eta kaltetutako produkturen batean batera pribilegiorik ez duen erasotzaile batek bereziki diseinatutako artxibo bat sortu lezake, ibilbide espezifiko batean, OpenSSL motor maltzur bat kargatzeko eta SYSTEM moduko kode arbitrarioa exekutatzeko, zerbitzua hasten denean. Horrela, erasotzailea administrari gisa sartuko litzateke sisteman, eta datu eta instalatutako aplikazio guztietarako sarbidea izango luke. Sistema Active Directory-ren domeinuaren kontrolatzaile bat ere bada, horrek domeinu osoari eragin ahal dio.

Ahultasun horretarako CVE-2019-12572 identifikatzailea esleitu da (Backup Exec. Produktuan).

Etiketak: Eguneratzea, SSL/TLS, Ahultasuna

DDoS eraso zabaldua Citrix ADC eta Gateway erakundeen aurka

Argitalpen data: 2020/12/28

Garrantzia: Handia

Kaltetutako baliabideak:

- Citrix ADC (*Application Delivery Controller*),
- Citrix Gateway.

Une honetan, erasoaren norainokoa mundu osoko bezero gutxi batzuetara mugatzen da.

Azalpena:

Citrix ha detectado un patrón de ataques DDoS que están utilizando el protocolo DTLS (*Datagram Transport Layer Security*)

como vector de amplificación.

Konponbidea:

Citrix erakundea DTLS protokoloaren ezaugarriak hobetzeko ari da lanean, eraso horren mende ez egoteko, eta espero du hobekuntza hori prest egotea 2021eko urtarrilaren 12rako, bertsio guztietarako, Citrixen deskarga-orrian. Une horretara arte, CLI komandoaren bidez DTLS desgaitzea gomendatu da:

```
set vpn vserver < vpn_vserver_name > -dtls OFF
```

EDT behar duen (*Enlightened Data Transport*) aplikazioaren bat exekutatzen ari bazara edo ezin baduzu DTLS desaktibatu, jarri harremanetan Citrixen talde teknikoarekin.

Xehetasuna:

Erasotzaile batek Citrix ADC-ren DTLS sarearen errendimendua gehiegi kargatu lezake, eta, horren ondorioz, irteerako bandaren zabalera agortu liteke. Eraso horren eragina handiagoa izan liteke zabalera mugatuko banda batekin. ADC bat eraso horren helburua den zehazteko, irteera-trafikoaren bolumena monitorizatu behar da, edozein gauza arraro edo piko antzemateko.

Etiketak: Komunikazioak