2020ko Urriaren Bulletina

Ohartarazpenak - Teknikoak

Hainbat ahultasun HPE IP Console Switch G2 4x1Ex32 sisteman

Argitalpen data: 2020/10/01

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HPE KVM IP Console Switches G2 4x1Ex32, 2.8.3 bertsioaren aurrekoak.

Azalpena:

Nikita Medvedev, Yandex etxeko ikertzaileak, 2 ahultasunen berri eman du, biak larritasun kritikokoak, XSS biltegiratuaren eta kodearen urrutiko exekuzioaren motakoak.

Konponbidea:

Produktua eguneratzea 2.8.3 bertsiora.

Xehetasunak:

Urrutiko erasotzaile batek ahultasunak baliatu litzake XSS (Cross-Site Scripting) biltegiratuaren erasoak edo kode exekuzioak (RCE) burutzeko. Ahultasun horietarako CVE-2020-24627 eta CVE-2020-24628 identifikatzaileak erreserbatu dira.

Etiketak: Eguneratzea, HP, Ahultasuna

Hainbat ahultasun Microsoft Azure Sphere sisteman

Argitalpen data: 2020/10/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Microsoft Azure Sphere, 20.06 eta 20.07 bertsioak.

Azalpena:

Cisco Talos erakundeko Lilith Wyatt, Claudio Bozzato eta Dave McDaniel ikertzaileek 4 ahultasun antzeman dituzte, 2 larritasun kritikokoak, bat handikoa eta bestea tartekoa. Motak: zerbitzu-ukapena, informazio-ihesa, kodearen exekuzioa eta memoria ustelkeria.

Konponbidea:

Cisco Talos erakundeko ikertzaileek ez dute oraindik konponbiderik zehaztu, baina gomendagarria da eskuragarri dagoen azken bertsioaren arabera produktuak eguneratzea; une honetan, 20.08 bertsioa da hori.

Xehetasunak:

- Zerbitzu ukapen motako ahultasun bat dago (DoS) Microsoft Azure Sphere 20.06 sistemaren Littlefs Quota

funtzionalitatean. Sistemara egindako bereziki diseinatutako dei multzo batek kuota omititzea eta berrabiaraztea eragin lezake. Erasotzaile batek deiak egin litzake sistemara, ahultasun hori aktibatzeko.
- SIGN_WITH_TENANT_ATTESTATION_KEY funtzionalitatearen ustelkeria ahultasun bat dago, Microsoft Azure Sphere 20.07 bertsioaren kernel /dev/pluton kontrolatzaileari dagokiona. Bereziki diseinatutako ioctl dei-sekuentzia batek kalteak eragin litzake memorian Plutonen. Erasotzaile batek ioctl dei bat egin lezake Normal World sistematik, ahultasun hori eragiteko.

Kritikoak ez diren gainerako ahultasun motak: Memoria dibulgazioa eta kodearen exekuzioa.

Etiketak: 0day, IoT, Microsoft, Ahultasuna.

Hainbat ahultasun HP Device Manager sisteman

Argitalpen data: 2020/10/07

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HP Device Manager sistemaren bertsio guztiak.

Azalpena:

Nick Bloor segurtasun ikertzaileak 3 ahultasunen berri eman dio HP PRST taldeari (Product Security Response Team). Bat larritasun kritikokoa da, eta beste biak handikoak. Motak: urrutiko metodoaren inbokazioa, zifratze ahula eta pribilegioen eskalatzea.

Konponbidea:

- HP Device Manager 4.7: laster Service Pack 13 argitaratuko da, ahultasun horiek konpontzeko;
- HP Device Manager 5.0: 5.0.4 bertsiora eguneratzea.

Xehetasunak:

- Ahultasun horren bidez, urrutiko erasotzaile bat baliabideetara sar liteke, baimenik gabe. Ahultasun kritiko horretarako, CVE-2020-6926 identifikatzailea esleitu da.
- Ahultasun horren bidez, HP Device Manager sistemaren barruan modu lokalean administratutako kontuek hiztegi erasoak izan litzakete, zifratze ahularen inplementazio baten ondorioz. Active Directory sistemako baimendutako kontuak erabiltzen dituzten bezeroei ez die eragiten. Ahultasun horretarako, CVE-2020-6925 identifikatzailea esleitu da.
- Ahultasun horren bidez, erasotzaile batek SYSTEM pribilegioak lortu litzake. Kanpo datu-base bat erabiltzen duten (Microsoft SQL Server), eta Postgres zerbitzu integratua instalatu ez duten bezeroei ez die eragiten. Ahultasun horretarako, CVE-2020-6927 identifikatzailea esleitu da.

Etiketak: Eguneratzea, HP, Ahultasuna

Hainbat ahultasun QNAP markaren Helpdesk sisteman

Argitalpen data: 2020/10/09

Garrantzia: Kritikoa

Kaltetutako baliabideak:

QNAP Helpdesk, 3.0.3 bertsioaren aurrekoak.

Azalpena:

Jose Antonio Pérez Piedrak QNAP gailuei eragiten dieten 2 ahultasunen berri eman du, biak larritasun kritikokoak.

Konponbidea:

Helpdesk sistema 3.0.3 bertsiora edo ostekoetara eguneratzea, QNAPen oharraren Updating Helpdesk ataleko jarraibideen arabera.

Xehetasunak:

- Sarbide-kontrol desegokiaren motako ahultasun horren bidez, erasotzaileek QNAP gailu baten kontrola lortu lezakete. Ahultasun horretarako, CVE-2020-2506 identifikatzailea esleitu da.
- Sarbide-kontrol desegokiaren motako ahultasun horren bidez, erasotzaileek QNAP gailu baten kontrola lortu lezakete. Ahultasun horretarako, CVE-2020-2507 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Pribatutasuna, Ahultasuna.

Pribilegioen eskalatze motako hainbat ahultasun

Acronis True Image, Cyber ??Backup eta Cyber ?? Protection sistemetan

Argitalpen data: 2020/10/13

Garrantzia: Altua

Kaltetutako baliabideak:

Hauen aurreko bertsioak:

- Acronis True Image 2021 build 32010,
- Acronis Cyber ??Backup 12.5 build 16363,
- Acronis Cyber ??Protect 15 build 24600.

Azalpena:

CERT/CC erakundeko ikertzaileek eta HackerOne erakundeko independenteek DLLren bilaketa-bahiketa motako hainbat ahultasunen berri eman diote Acronis etxeari. Ahultasun horien bidez, sistemarako sarbide lokala duen erasotzaile batek programaren hasieran kargatzen diren konfigurazio fitxategiak eta DLL fitxategiak alda litzake, Windows eremuan pribilegio eskalatzea eraginez, eta SYSTEM pribilegioekin kodea exekutatzea ahalbidetuz.

Konponbidea:

Honako ahultasunak konpontzeko bertsio hauek instalatzea gomendatzen da:

- Acronis True Image 2021 build 32010,
- Acronis Cyber ??Backup 12.5 build 16363,
- Acronis Cyber ??Protect 15 build 24600.

Xehetasunak:

DLL bilaketa bahiketaren motako hiru ahultasun antzeman dira. Horien bidez, sistemarako sarbide lokala duen erasotzaile batek DLL fitxategiak eta konfiguraziokoak alda litzake, SYSTEM pribilegioekin eskalatze bat eraginez.

- Pribilegiorik ez duten Windows erabiltzailek azpidirektorioak sortu ditzakete sistemaren errotik kanpo, beraz, erabiltzaile batek ibilbide egokia sortu lezake C:jenkins_agent-en barruan, bereziki diseinatutako openssl.cnf fitxategi bat kargatu eta kodea pribilegioekin exekutatzeko. Ahultasun horrek Acronisen 3 produkturi eragiten die eta CVE-2020-10138 eta CVE-2020-10139 identifikatzaileak esleitu zaizkie.
- Acronis True Image 2021ek ez ditu ondo konfiguratzen ACL delakoak C:ProgramDataAcronis ibilbidean, beraz, pribilegiorik gabeko erabiltzaile batek kode arbitrarioa exekuta lezake pribilegioekin, ibilbide horren barruan DLL eraldatu bat jarriz. Ahultasun horretarako, CVE-2020-10140 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna, Windows.

Microsoften segurtasun buletina. 2020ko urria

Argitalpen data: 2020/10/14

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Microsoft Windows;
- Microsoft Office, Microsoft Office Services eta Web Apps;
- Microsoft JET Database Engine;
- Azure Functions;
- Open Source Software;
- Microsoft Exchange Server;
- Visual Studio;
- PowerShellGet;
- Microsoft .NET Framework;
- Microsoft Dynamics;
- Adobe Flash Player;
- Microsoft Windows Codecs Library.

Azalpena:

Segurtasun eguneratzeen inguruko urriko Microsoft argitalpenean 83 ahultasun jaso dira oraingoan; 11 kritiko gisa sailkatu dira eta 72 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,
- Kodearen urrutiko exekuzioa.
- Informazioa zabaltzea.
- Zerbitzua ukatzea.

- Segurtasun-neurriak saihestea,
- Nortasuna ordeztea (spoofing).

Etiketak: Eguneratzea, Adobe, Komunikazioak, Microsoft, Ahultasuna, Windows

---

Hainbat ahultasun Juniper produktuetan

Argitalpen data: 2020/10/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Junos OS, bertsio hauek: 12.3, 12.3X48, 15.1, 15.1X49, 16.1, 17.2, 17.2X75, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2, 19.3 y 19.4, 20.1;
- Mist Cloud UI;
- Contrail Networking.

Azalpena:

Juniperrek hainbat ahultasunetarako segurtasun oharrak argitaratu ditu. Horien artean, nabarmendu beharko genituzke larritasun kritikoko 3, mota hauetakoak: Telnet zerbitzariko kodearen exekuzio arbitrarioa, SAML erantzunen kudeaketa desegokia eta exekuzio arbitrarioa YAML artxibo ez fidagarriak prozesatzean.

Konponbidea:

- Juno OS bertsio hauetakoren batera eguneratzea: 12.3R12-S16, 12.3X48-D105, 15.1R7-S7, 15.1X49-D220, 15.1X49-D230, 16.1R7-S8, 17.2R3-S4, 17.2X75-D45, 17.3R3-S8, 17.3R3-S9, 17.4R2-S11, 17.4R3-S2, 18.1R3-S10, 18.2R3-S5, 18.2X75-D34, 18.2X75-D41, 18.2X75-D430, 18.2X75-D65, 18.3R2-S4, 18.3R3-S3, 18.4R2-S5, 18.4R3-S4, 19.1R2-S2, 19.1R3-S2, 19.2R1-S5, 19.2R2, 19.2R2-S1, 19.2R3, 19.3R2-S3, 19.3R3, 19.4R1-S3, 19.4R2-S1, 19.4R3, 20.1R1-S2, 20.1R2, 20.2R1, 20.3X75-D10 eta ostekoak;
- Mist Cloud UI 2020ko irailaren 2an eguneratu zen, ahultasunak konpontzeko;
- Contrail Networking R2008 bertsiora eguneratzea.

Eguneratze guztiak eskura daude Juniperren deskarga zentroan.

Xehetasunak:

- Telnet telnetd zerbitzariko ahultasun baten bidez, urrutiko erasotzaileek kode arbitrarioa exekutatu lezakete idazketa labur edo datu urgenteen bidez, netclear eta nextitem funtzioak barne hartzen dituen buffer gainezkatzearen bidez. Ahultasun horretarako, CVE-2020-10188 identifikatzailea esleitu da.
- Mist Cloud UI sistemak, SAML egiaztatzea gaituta dagoenean, SAML erantzunak desegoki kudeatu litzake (Security Assertion Markup Language), eta urrutiko erasotzaile batek SAML egiaztatzearen segurtasun kontrolak saihestu litzake. CVE-2020-1675, CVE-2020-1676 y CVE-2020-1677 identifikatzaileak esleitu dira ahultasun horietarako. Bakarrik edota konbinatuta ustiatu daitezke.
- PyYAML liburutegiko ahultasun baten bidez, kode arbitrarioa exekutatu liteke konfiantzazkoak ez diren YAML artxiboak prozesatzean (YAML Ain't Markup Language), full load metodoaren bidez edo FullLoader kargadorearen bidez. Ahultasun horretarako, CVE-2020-1747 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

2020ko urriko SAP segurtasunaren eguneratzea

Arigtalpen data: 2020/10/15

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- SAP Solution Manager eta SAP Focused Run, 9.7, 10.1, 10.5 eta 10.7 bertsioak;
- SAP Business Client, 6.5 bertsioa;
- SAP NetWeaver, 7.00, 7.01, 7.02, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, 7.51, 7.53 eta 7.55 bertsioak;
- SAP Business Objects Business Intelligence Platform, 4.1, 4.2 eta 4.3 bertsioak;
- SAP Landscape Management, 3.0 bertsioa;
- SAP Adaptive Extensions, 1.0 bertsioa;
- SAP 3D Visual Enterprise Viewer, 9 bertsioa;
- SAP Commerce Cloud, 1808, 1811, 1905 eta 2005 bertsioak;
- SAP Business Planning y Consolidation, 750, 751, 752, 753, 754, 755, 810, 100 eta 200 bertsioak;
- SAP ERP (HCM Travel Management); 600, 602, 603, 604, 605, 606, 607 eta 608 bertsioak;
- SAP Banking Services, 500 bertsioa.

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, segurtasun-partxeen hileroko komunikazioan, 15 segurtasun ohar eta eguneratze 6 egin ditu. Horietako 2 larritasun kritikokoak dira, 7 altukoa, 11 tartekoak eta 1 baxukoa.

Argitaratutako ahultasun mota berriak honakoekin bat datoz:

- XSS motako 6 ahultasun (Cross-Site Scripting),
- Informazioaren dibulgazioaren arloko 3 ahultasun,
- Kodearen injekzioaren kontrol ahultasun bat,
- Baimen konprobatze faltaren ahultasun bat,
- XML balioztatze faltaren ahultasun bat,
- Kredentzial barneratuen ahultasun bat,
- SSOO komandoetako injekzioaren motako ahultasun bat,
- Beste motaren bateko 12 ahultasun.

Segurtasun ohar nabarmenenak honakoen ingurukoak dira:

- Ahultasun horren bidez, erasotzaile batek sistema eragilearen komandoak injektatu litzake eta CA Introscope Enterprise Manager exekutatzen duen host osoaren kontrola eskuratu. Ahultasun horretarako, CVE-2020-63640 identifikatzailea esleitu da.
- 2018ko apirileko segurtasun-oharra eguneratzea, SAP Business Client sistemarekin entregatutako Google Chromium nabigatzailearen kontrolerako.

Gainerako ahultasunetarako, honako identifikatzaileak erreserbatu dira: CVE-2020-6296, CVE-2020-6367, CVE-2020-6366, CVE-2020-6369, CVE-2020-6309, CVE-2020-6237, CVE-2020-6236, CVE-2020-6319, CVE-2020-6315, CVE-2020-6372, CVE-2020-6373, CVE-2020-6374, CVE-2020-6375, CVE-2020-6376, CVE-2020-6272, 6368, CVE-2020-6301, CVE-2020-6308, CVE-2020-6370, CVE-2020-6365, CVE-2020-6323, CVE-2020-6371, CVE-2020-6362 eta CVE-2020-6363.

Etiketak: Eguneratzea, SAP, Ahultasuna

Kodearen urrutiko exekuzioa Visual Studio eta Microsoft Windows Codecs Library sistemetan

Argitalpen data: 2020/10/19

Garrantzia: Altua

Kaltetutako baliabideak:

- Windows 10, 1709 bertsioa 32 biteko sistemetarako,
- Windows 10, 1709 bertsioa ARM64 oinarria duten sistemetarako,
- Windows 10, 1709 bertsioa x64 oinarria duten sistemetarako,
- Windows 10, 1803 bertsioa 32 biteko sistemetarako,
- Windows 10, 1803 bertsioa ARM64 oinarria duten sistemetarako,
- Windows 10, 1803 bertsioa x64 oinarria duten sistemetarako,
- Windows 10, 1809 bertsioa 32 biteko sistemetarako,
- Windows 10, 1809 bertsioa ARM64 oinarria duten sistemetarako,
- Windows 10, 1809 bertsioa x64 oinarria duten sistemetarako,
- Windows 10, 1903 bertsioa 32 biteko sistemetarako,
- Windows 10, 1903 bertsioa ARM64 oinarria duten sistemetarako,
- Windows 10, 1903 bertsioa x64 oinarria duten sistemetarako,
- Windows 10, 1909 bertsioa ARM64 oinarria duten sistemetarako,
- Windows 10, 1909 bertsioa x64 oinarria duten sistemetarako,
- Windows 10, 2004 bertsioa 32 biteko sistemetarako,
- Windows 10, 2004 bertsioa ARM64 oinarria duten sistemetarako,
- Windows 10, 2004 bertsioa x64 oinarria duten sistemetarako,
- Visual Studio Code.

Azalpena:

Microsoftek bi segurtasun-abisu argitaratu ditu kaltetutako produktuetan kodearen urrutiko exekuzioari dagozkion ahultasunak zuzentzeko.

Konponbidea:

- Windows Media Codec-erako eguneratzeak zuzendu egiten du Microsoft Windows Codecs Library sistemak objektuak memorian erabiltzeko daukan modua. Kaltetutako bezeroek automatikoki eguneratuko dute Microsoft Store bidez.
- Visual Studiorako, azken bertsioa deskargatu behar da, Visual Studioren kodeak JSON artxiboak erabiltzen dituen modua aldatzen baitu.

Xehetasunak:

- Microsoft Windowsen kodek liburutegiko ahultasun batek, objektuak memorian erabilita, erasotzaile bati kodea urrutitik exekutatzea eragin lezake, bereziki diseinatutako irudi artxibo baten prozesatzean. Ahultasun horretarako, CVE-2020-17022 identifikatzailea esleitu da.
- Visual Studio kodean agertzen den ahultasun baten bidez, erasotzaile batek kode arbitrarioa exekuta lezake egungo erabiltzailearen testuinguruan, erabiltzaile hori engainatzen badu biltegi bat klonatzeko eta 'package.json' artxibo maltzur bat irekitzeko. Ahultasun horretarako, CVE-2020-17023 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Microsoft, Ahultasuna, Windows.

Pilan oinarritutako buffer gainezkatzea SonicWall SonicOS sisteman

Argitalpen data: 2020/10/20

Garrantzia: Kritikoa

Kaltetutako baliabideak:

SonicOS, bertsioak:

- 6.5.4.6-79n eta aurrekoak;
- 6.5.1.11-4n eta aurrekoak;
- 6.0.5.3-93o eta aurrekoak;
- 6.5.4.4-44v-21-794 eta aurrekoak;
- 7.0.0.0-1.
- .

Azalpena:

Positive Technologies enpresako Nikita Abramov eta Tripwire enpresako Craig Young ikertzaileek SonicWall sistema eragilearen SonicOS tresnaren hainbat bertsiori eragiten dien larritasun kritikoko ahultasun bat antzeman dute.

Konponbidea:

- SonicOS bertsio hauetakoren batera eguneratzea:
  - 6.5.4.7-83n;
  - 6.5.1.12-1n;
  - 6.0.5.3-94o;
  - 6.5.4.v-21s-987;
  - 7 7.0.0.0-2 edo ostekoak.

Xehetasunak:

Pilan oinarritutako buffer gainezkatzearen motako (stack) ahultasun bat antzeman da SonicOS tresnan. Horren bidez, urrutiko erasotzaile batek, baimenik gabe, zerbitzu ukapena eragin lezake (DoS), eta kode arbitrarioa exekutatu, firewall-era eskaera maltzurra bidaliz. Ahultasun horretarako, CVE-2020-5135 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Pribatutasuna, Ahultasuna.

Eguneraketa kritikoak Oraclen (2020ko urria)

Argitalpen data: 2020/10/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Application Performance Management (APM), 13.3.0.0, 13.4.0.0 bertsioak;
- Big Data Spatial and Graph, 3.0ren aurreko bertsioak;
- Enterprise Manager Base Platform, 13.2.1.0, 13.3.0.0, 13.4.0.0 bertsioak;
- Enterprise Manager for Peoplesoft, 13.4.1.1 bertsioa;
- Enterprise Manager for Storage Management, 13.3.0.0, 13.4.0.0 bertsioak;
- Enterprise Manager Ops Center, 12.4.0.0 bertsioa;
- Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, XCP2362 eta XCP3090ren aurreko bertsioak;
- Fujitsu M12-1, M12-2, M12-2S Servers, XCP3090ren aurreko bertsioak;
- Hyperion Analytic Provider Services, 11.1.2.4 bertsioa;
- Hyperion BI , 11.1.2.4 bertsioa;
- Hyperion Essbase, 11.1.2.4 bertsioa;
- Hyperion Infrastructure Technology, 11.1.2.4 bertsioa;
- Hyperion Lifecycle Management, 11.1.2.4 bertsioa;
- Hyperion Planning, 11.1.2.4 bertsioa;
- Identity Manager Connector, 9.0 bertsioa;
- Instantis EnterpriseTrack, 17.1, 17.2, 17.3 bertsioak;
- Management Pack for Oracle GoldenGate, 12.2.1.2.0 bertsioa;
- MySQL Cluster, 7.3.30 bertsioa eta aurrekoak, 7.4.29 bertsioa eta aurrekoak, 7.5.19 bertsioa eta aurrekoak, 7.6.15 bertsioa eta aurrekoak, 8.0.21 bertsioa eta aurrekoak;
- MySQL Enterprise Monitor, 8.0.21 bertsioa eta aurrekoak;
- MySQL Server, 5.6.49 bertsioa eta aurrekoak, 5.7.31 eta aurrekoak, 8.0.21 eta aurrekoak.
- MySQL Workbench, 8.0.21 bertsioa eta aurrekoak;
- Oracle Access Manager, 11.1.2.3.0 bertsioa;
- Oracle Agile PLM, 9.3.3, 9.3.5, 9.3.6 bertsioak;
- Oracle Agile Product Lifecycle Management for Process, 6.2.0.0 bertsioa;
- Oracle Application Express, 20.2 bertsioaren aurrekoak;
- Oracle Application Testing Suite, 13.3.0.1 bertsioa;
- Oracle Banking Corporate Lending, 12.3.0, 14.0.0-14.4.0 bertsioak;
- Oracle Banking Digital Experience, 18.1, 18.2, 18.3, 19.1, 19.2, 20.1 bertsioak;
- Oracle Banking Payments, 14.1.0-14.4.0 bertsioak;
- Oracle Banking Platform, 2.4.0-2.10.0 bertsioak;
- Oracle BI Publisher, 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Business Intelligence Enterprise Edition, 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Business Process Management Suite, 12.2.1.3.0, 12.2.1.4.0 bertsioak;

- Oracle Communications Application Session Controller, 3.8m0, 3.9m0p1 bertsioak;
- Oracle Communications Billing and Revenue Management, 7.5.0.23.0, 12.0.0.2.0, 12.0.0.3.0 bertsioak;
- Oracle Communications BRM - Elastic Charging Engine, 11.3.0.9.0, 12.0.0.3.0 bertsioak;
- Oracle Communications Diameter Signaling Router (DSR), 8.0.0.0-8.4.0.5, [IDIH] 8.0.0-8.2.2 bertsioak;
- Oracle Communications EAGLE Software, 46.6.0-46.8.2 bertsioak;
- Oracle Communications Element Manager, 8.2.0-8.2.2 bertsioak;
- Oracle Communications Evolved Communications Application Server, 7.1 bertsioa;
- Oracle Communications Messaging Server, 8.1 bertsioa;
- Oracle Communications Offline Mediation Controller, 12.0.0.3.0 bertsioa;
- Oracle Communications Services Gatekeeper, 7 bertsioa;
- Oracle Communications Session Border Controller, 8.2-8.4 bertsioak;
- Oracle Communications Session Report Manager, 8.2.0-8.2.2 bertsioak;
- Oracle Communications Session Route Manager, 8.2.0-8.2.2 bertsioak;
- Oracle Communications Unified Inventory Management, 7.3.0, 7.4.0 bertsioak;
- Oracle Communications WebRTC Session Controller, 7.2 bertsioa;
- Oracle Data Integrator, 11.1.1.9.0, 12.2.1.3.0 bertsioak;
- Oracle Database Server, 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c bertsioak;
- Oracle E-Business Suite, 12.1.1-12.1.3, 12.2.3-12.2.10 bertsioak;
- Oracle Endeca Information Discovery Integrator, 3.2.0 bertsioa;
- Oracle Endeca Information Discovery Studio, 3.2.0 bertsioa;
- Oracle Enterprise Repository, 11.1.1.7.0 bertsioa;
- Oracle Enterprise Session Border Controller, 8.4 bertsioa;
- Oracle Financial Services Analytical Applications Infrastructure, 8.0.6-8.1.0 bertsioak;
- Oracle Financial Services Analytical Applications Reconciliation Framework, 8.0.6-8.0.8, 8.1.0 bertsioak;
- Oracle Financial Services Asset Liability Management, 8.0.6, 8.0.7, 8.1.0 bertsioak;
- Oracle Financial Services Balance Sheet Planning, 8.0.8 bertsioa;
- Oracle Financial Services Basel Regulatory Capital Basic, 8.0.6-8.0.8, 8.1.0 bertsioak;
- Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach, 8.0.6-8.0.8, 8.1.0 bertsioak;
- Oracle Financial Services Data Foundation, 8.0.6-8.1.0 bertsioak;
- Oracle Financial Services Data Governance for US Regulatory Reporting, 8.0.6-8.0.9 bertsioak;
- Oracle Financial Services Data Integration Hub, 8.0.6, 8.0.7, 8.1.0 bertsioak;
- Oracle Financial Services Funds Transfer Pricing, 8.0.6, 8.0.7, 8.1.0 bertsioak;
- Oracle Financial Services Hedge Management and IFRS Valuations, 8.0.6-8.0.8, 8.1.0 bertsioak;
- Oracle Financial Services Institutional Performance Analytics, 8.0.6, 8.0.7, 8.1.0, 8.7.0 bertsioak;
- Oracle Financial Services Liquidity Risk Management, 8.0.6 bertsioa;
- Oracle Financial Services Liquidity Risk Measurement and Management, 8.0.7, 8.0.8, 8.1.0 bertsioak;
- Oracle Financial Services Loan Loss Forecasting and Provisioning, 8.0.6-8.0.8, 8.1.0 bertsioak;
- Oracle Financial Services Market Risk Measurement and Management, 8.0.6, 8.0.8, 8.1.0 bertsioak;
- Oracle Financial Services Price Creation and Discovery, 8.0.6, 8.0.7 bertsioak;
- Oracle Financial Services Profitability Management, 8.0.6, 8.0.7, 8.1.0 bertsioak;
- Oracle Financial Services Regulatory Reporting for European Banking Authority, 8.0.6-8.1.0 bertsioak;
- Oracle Financial Services Regulatory Reporting for US Federal Reserve, 8.0.6-8.0.9 bertsioak;
- Oracle Financial Services Regulatory Reporting with AgileREPORTER, 8.0.9.2.0 bertsioa;
- Oracle Financial Services Retail Customer Analytics, 8.0.6 bertsioa;
- Oracle FLEXCUBE Core Banking, 5.2.0, 11.5.0-11.7.0 bertsioak;
- Oracle FLEXCUBE Direct Banking, 12.0.1, 12.0.2, 12.0.3 bertsioak;
- Oracle FLEXCUBE Private Banking, 12.0.0, 12.1.0 bertsioak;
- Oracle FLEXCUBE Universal Banking, 12.3.0, 14.0.0-14.4.0 bertsioak;
- Oracle GoldenGate Application Adapters, 12.3.2.1.0, 19.1.0.0.0 bertsioak;
- Oracle GraalVM Enterprise Edition, 19.3.3, 20.2.0 bertsioak;
- Oracle Health Sciences Empirica Signal, 9.0 bertsioa;
- Oracle Healthcare Data Repository, 7.0.1 bertsioa;
- Oracle Healthcare Foundation, 7.1.1, 7.2.0, 7.2.1, 7.3.0 bertsioak;
- Oracle Hospitality Guest Access, 4.2.0, 4.2.1 bertsioak;
- Oracle Hospitality Materials Control, 18.1 bertsioa;
- Oracle Hospitality OPERA 5 Property Services, 5.5, 5.6 bertsioak;
- Oracle Hospitality Reporting and Analytics, 9.1.0 bertsioa;
- Oracle Hospitality RES 3700, 5.7 bertsioa;
- Oracle Hospitality Simphony, 18.1, 18.2, 19.1.0-19.1.2 bertsioak;
- Oracle Hospitality Suite8, 8.10.2, 8.11-8.15 bertsioak;
- Oracle HTTP Server, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Insurance Accounting Analyzer, 8.0.9 bertsioa;
- Oracle Insurance Allocation Manager for Enterprise Profitability, 8.0.8, 8.1.0 bertsioak;
- Oracle Insurance Data Foundation, 8.0.6-8.1.0 bertsioak;
- Oracle Insurance Insbridge Rating and Underwriting, 5.0.0.0-5.6.0.0, 5.6.1.0 bertsioak;
- Oracle Insurance Policy Administration J2EE, 10.2.0.37, 10.2.4.12, 11.0.2.25, 11.1.0.15, 11.2.0.26, 11.2.2.0 bertsioak;
- Oracle Insurance Rules Palette, 10.2.0.37, 10.2.4.12, 11.0.2.25, 11.1.0.15, 11.2.0.26 bertsioak;
- Oracle Java SE, 7u271, 8u261, 11.0.8, 15 bertsioak;
- Oracle Java SE Embedded, 8u261 bertsioa;
- Oracle JDeveloper, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Managed File Transfer, 12.2.1.3.0, 12.2.1.4.0 bertsioak;
- Oracle Outside In Technology, 8.5.4, 8.5.5 bertsioak;
- Oracle Policy Automation, 12.2.0-12.2.20 bertsioak;
- Oracle Policy Automation Connector for Siebel, 10.4.6 bertsioa;
- Oracle Policy Automation for Mobile Devices, 12.2.0-12.2.20 bertsioak;
- Oracle REST Data Services, 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c, [Standalone ORDS] bertsioak 20.2.1aren aurrekoak;
- Oracle Retail Advanced Inventory Planning, 14.1 bertsioa;
- Oracle Retail Assortment Planning, 15.0.3.0, 16.0.3.0 bertsioak;
- Oracle Retail Back Office, 14.0, 14.1 bertsioak;
- Oracle Retail Bulk Data Integration, 15.0.3.0, 16.0.3.0 bertsioak;
- Oracle Retail Central Office, 14.0, 14.1 bertsioak;
- Oracle Retail Customer Management and Segmentation Foundation, 18.0, 19.0 bertsioak;
- Oracle Retail Integration Bus, 14.1, 15.0, 16.0 bertsioak;
- Oracle Retail Order Broker, 15.0, 16.0, 18.0, 19.0, 19.1, 19.2, 19.3 bertsioak;
- Oracle Retail Point-of-Service, 14.0, 14.1 bertsioak;
- Oracle Retail Predictive Application Server, 14.1.3.0, 15.0.3.0, 16.0.3.0 bertsioak;
- Oracle Retail Price Management, 14.0.4, 14.1.3.0, 15.0.3.0, 16.0.3.0 bertsioak;

- Oracle Retail Returns Management, 14.0, 14.1 bertsioak;
- Oracle Retail Service Backbone, 14.1, 15.0, 16.0 bertsioak;
- Oracle Retail Xstore Point of Service, 15.0.3, 16.0.5, 17.0.3, 18.0.2, 19.0.1 bertsioak;
- Oracle Solaris, 10, 11 bertsioak;
- Oracle TimesTen In-Memory Database, 11.2.2.8.49, 18.1.3.1.0 bertsioak, eta 18.1.4.1.0 bertsioaren aurrekoak;
- Oracle Transportation Management, 6.3.7 bertsioa;
- Oracle Utilities Framework, 2.2.0.0.0, 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0 bertsioak;
- Oracle VM VirtualBox, 6.1.16 bertsioaren aurrekoak;
- Oracle WebCenter Portal, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 bertsioaren aurrekoak;
- Oracle WebLogic Server, 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0 bertsioak;
- Oracle ZFS Storage Appliance Kit, 8.8 bertsioa;
- PeopleSoft Enterprise HCM Global Payroll Core, 9.2 bertsioa;
- PeopleSoft Enterprise PeopleTools, 8.56, 8.57, 8.58 bertsioak;
- PeopleSoft Enterprise SCM eSupplier Connection, 9.2 bertsioa;
- Primavera Gateway, 16.2.0-16.2.11, 17.12.0-17.12.8 bertsioak;
- Primavera Unifier, 16.1, 16.2, 17.7-17.12, 18.8, 19.12 bertsioak;
- Siebel Applications, 20.7, 20.8 bertsioak.

Azalpena:

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

Konponbidea:

Kaltetutako produktuen araberako partxeak aplikatzea. Eguneraketak deskargatzeko informazioa Oraclek argitaratutako segurtasun buletinean eskura daiteke.

Xehetasunak:

Eguneraketa horrek 402 ahultasun konpontzen ditu, horietako batzuk kritikoak. Konpondutako ahultasunen xehetasuna Oracleren loturan dagoen Erreferentzien atalean kontsulta daiteke.

Etiketak: Eguneratzea, Java, Oracle, Ahultasuna

Hainbat ahultasun VMware produktuetan

Argitalpen data: 2020/10/21

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- ESXi, 6.7 eta 6.5 bertsioak;
- Workstation Pro / Player (Workstation), 15.x bertsioa;
- Fusion Pro / Fusion (Fusion), 11.x bertsioa (OS X sisteman exekutatzen);
- NSX-T, 3.x eta 2.5.x bertsioak;
- Cloud Foundation, bertsioak: 4.x (CVE-2020-3992, CVE-2020-3993, CVE-2020-3981 eta CVE-2020-3982 ahultasunetarako) eta 3.x;
- vCenter Server, bertsioak: 6.7 (Virtual Appliance sisteman exekutatzen) eta 6.5 (Virtual Appliance sisteman exekutatzen).

Azalpena:

Hainbat ikertzailek VMware 6 sistemari eman diote 6 ahultasunen berri, bata larritasun kritikokoa, 4 handikoak eta bat tartekoa. Motak: aurretik liberatutako memoriaren erabilera, MitM (man in the middle), mugaz kanpoko irakurketa, saioa bahitzea (hijacking), mugaz kanpoko irakurketa eta memoria galera.

Konponbidea:

Kaltetutako produktuetarako azken partxeak instalatzea gomendatzen da, erabilitako bertsio egonkorraren arabera, dagokion Response Matrix taularen Fixed Version atalean adierazi bezala.

Xehetasunak:

Larritasun kritikoko ahultasun honen bidez, ESXi makina batean 427 portura eta administrazio sarera sarbidea duen erasotzaile batek kodearen urrutiko exekuzioa burutu lezake, OpenSLP zerbitzuan aurretik liberatutako memoriaren motako ahultasuna baliatuz. Ahultasun horretarako, CVE-2020-3992 identifikatzailea esleitu da.

Gainerako ahultasunerako esleitutako beste identifikatzaile batzuk: CVE-2020-3981, CVE-2020-3982, CVE-2020-3993, CVE-2020-3994 eta CVE-2020-3995.

Etiketak: Eguneratzea, Birtualizazioa, VMware, Ahultasuna.

Informazio pribilegiatuaren ahultasuna hainbat HPE produktutan

Argitalpen data: 2020/10/22

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- BlueData EPIC Software, 4.0 bertsioa eta aurrekoak;
- HPE Ezmeral Container Platform, 5.0 bertsioa.

Azalpena:

Early Warning Security erakundeko Hamoon Raphael Mehran ikertzaileak larritasun kritikoko ahultasun baten berri eman du. Mota: informazio pribilegiatuaren urruneko zabalkundearen motakoa.

Konponbidea:

- BlueData EPIC Software Platform sistemaren 4.0 bertsioak ahultasun hori konpontzeko partxe bat dauka. HPEren laguntza taldearekin harremanetan jartzea, hori lortzeko;
- HPE Ezmeral Container Platform 5.1 bertsiora edo ostekoetara eguneratzea.

Xehetasuna:

Ahultasun horrek kaltetutako produktuek metodo ez segurua erabiltzen dute Kerberos pasahitzen kudeaketan, eta baliteke pasahitzak lapurtzea eta baimenik gabe erabiltzea. Zehazki, *kdc_admin_password* erakusten da */bdswebui/assignusers/* URLaren iturri-artxiboan. Ahultasun horretarako, CVE-2020-7196 identifikatzailea esleitu da.

Etiketak: Eguneratzea, HP, Ahultasuna

Pribilegioen eskalatzea Chocolatey Boxstarter sisteman

Argitalpen data: 2020/10/23

Garrantzia: Handia

Kaltetutako baliabideak:

Chocolatey Boxstarter, 2.12.0 bertsioa eta aurrekoak.

Azalpena:

Will Dormannek larritasun handiko ahultasun baten berri eman dio CERT/CC erakundeari. Horren bidez, erasotzaile batek pribilegioetan gora egin lezake Chocolatey Boxstarter sisteman.

Konponbidea:

2.13.0 bertsiora eguneratzea.

Xehetasuna:

Chocolatey Boxstarter sistemaren instalatzaileak akatsa egin du *C:ProgramDataBoxstarter* direktorioan sarbide seguruaren (ACL) kontrol-zerrenda bat ezartzean. Sistemaren PATH eremuaren aldagaiari gehitzen zaio hori. Ahultasun horren bidez, erasotzaile batek pribilegioen eskalatzea egin lezake, izan ere, *PATH* eremuaren aldagaiaren edozein kokapen pribilegioekin exekutatzen den kodea kargatzeko erabil daiteke. Ahultasun horretarako, CVE-2020-15264 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna

Urruneko egiaztatzearen omisioa HPE SSMC sisteman

Argitalpen data: 2020/10/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

HPE 3PAR StoreServ Management eta Core Software Media, 3.7.0.0 bertsioaren aurrekoak.

Azalpena:

MindPoint Group erakundeko Elwood Buck ikertzaileak larritasun kritikoko ahultasun baten berri eman dio HPEri. Urruneko egiaztatzearen omisio motakoa da, eta StoreServ Management Console (SSMC) produktuari eragiten dio.

Konponbidea:

- HPE 3PAR StoreServ Management Console 3.7.1.1 bertsiora edo ostekoetara eguneratzea;
- SSMC 3.7.1.1 bertsiora eguneratzea. Hemen dago eskuragarri: mylicense portal.

Xehetasuna:

HPE StoreServ Management Console (SSMC) multiarray administrariaren nodotik kanpoko web aplikazioa da; administratutako matrizeen datuetatik isolatuta geratzen da eta urrutiko egiaztatzearen omisioa gerta dakioke. Ahultasun horretarako, CVE-2020-7197 identifikatzailea esleitu da.

Etiketak: Eguneratzea, HP, Ahultasuna

Arubaren AirWave Glass sistemaren ahultasunak

Argitalpen data: 2020/10/26

Garrantzia: Kritikoa

Kaltetutako baliabideak:

AirWave Glass, 1.3.1 bertsioa eta aurrekoak.

Azalpena:

Arubaren AirWave Glass sisteman hainbat ahultasun argitaratu dira. Horien bidez, erasotzaile batek kodea urrutitik exekuta lezake, sistema guztiz konprometitu, pribilegioak handitu edota Server Side Request Forgery erasoak burutu.

Konponbidea:

Airwave Glass 1.3.2 bertsiora edo goragoko batera eguneratzea.

Xehetasuna:

- Edukiontzien kudeaketa zerbitzuak egiaztatu gabe erakusgai izanda, erasotzaile batek kodearen urrutiko exekuzioa burutu lezake. Ahultasun horietarako CVE-2020-7127 eta CVE-2020-7128 identifikatzaileak erreserbatu dira.
- Webgunearen kudeaketa interfazerako sarbidea duten erasotzaileek ahultasun bat baliatu lezakete edukiontziaren kudeaketa sisteman sartu eta sistema anfitrioia guztiz konprometitzeko. Ahultasun horretarako, CVE-2020-7124 identifikatzailea esleitu da.
- Sarbide kontrolaren balioztatze desegokiaren bidez, soilik irakurtzeko pribilegioak dituen erabiltzaile batek pribilegioetan gora egin lezake erabiltzaile berriak gehituta, edota pribilegio handienak dituzten erabiltzaileen propietateak aldatu. Ahultasun horretarako, CVE-2020-7125 identifikatzailea esleitu da.
- Glassadmin pribilegioak dituen erabiltzaile batek kode arbitrarioa exekuta lezake root gisa azpiko host-aren sistema eragilean, cristaladmin cli bidez. Ahultasun horietarako CVE-2020-7129, CVE-2020-24631 eta CVE-2020-24632 identifikatzaileak esleitu dira.
- Airwave Glass sistemak egiaztatu gabeko *endpoint* bat erakusten du Grafana azpisisteman. Hori erabili egin daiteke *Server Side Request Forgery* eraso bat lortzeko. Horrela, barne-sistemaren endpoint delakoen datuak filtratu daitezke. Ahultasun horretarako, CVE-2020-7126 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Pribilegioak handitzea Macrium Reflect sisteman

Argitalpen data: 2020/10/27

Garrantzia: Handia

Kaltetutako baliabideak:

Macrium Reflect, 7.3.5281 bertsioaren aurrekoak.

Azalpena:

CERT/CC erakundeko Will Dormannek larritasun handiko ahultasun baten berri eman du. Pribilegioen eskalatze motakoa da, *OPENSSLDIR* aldagaiaren erabilerak sortua. Kokapen bat zehazten du eta pribilegiorik gabeko Windows erabiltzaile batek artxiboak sortu ditzake.

Ebazpena:

Macrium Reflect bertsio honetara eguneratzea: 7.3.5281.

Xehetasuna:

Macrium Reflect-en barne hartutako OpenSSL osagai ahul baten bidez, pribilegiorik gabeko erasotzaile batek *SYSTEM* pribilegiodun kode arbitrarioa exekuta lezake, C:openssl direktorioan bereziki diseinatutako *openssl*.cnf artxibo baten kokapenaren bidez. Ahultasun horretarako, CVE-2020-10143 identifikatzailea esleitu da.

Etiketak: Eguneratzea, Ahultasuna, Windows.

Hainbat ahultasun Synology Router Manager sisteman

Argitalpen data: 2020/10/30

Garrantzia: Kritikoa

Kaltetutako baliabideak:

- Synology SRM, honako bertsioak:
  - 1.2.3 MR2200ac 8017 eta 1.2.3 RT2600ac 8017;
  - 6.2.3 25426 DS120j;
  - 1.2.3 RT2600ac 8017-5.
- Synology QuickConnect.

Azalpena:

Cisco Talos erakundeak hainbat ahultasun antzeman ditu Synology routerren softwareetan, Synology Router Manager (SRM) eta QuickConnect sistemetan. Urrutiko erasotzaile batek ahultasun horiek baliatu litzake ekintza maltzurrak burutzeko, hala nola kodearen urrutiko exekuzioa, biktimaren sareko informazio sentikorra zabaltzea, eta sare berean konektatutako beste gailu batzuekiko komunikazioa.

Konponbidea:

Snort arauak: 53755, 53756, 53839, 53840, 53959 eta 54009, ahultasun horiek baliatzeko saiakerak antzemateko erabil daitezke.

Xehetasunak:

Larritasun kritikoko ahultasun horren bidez, Synology SRM 1.2.3 RT2600ac 8017-5 bertsioan, Qualcomm lbd 1.1en lbd zerbitzuaren funtzionalitatean, erasotzaile batek modu arbitrarioan gainidatz ditzake bereziki diseinatutako depurazio komando baten bidez, eta kodearen urrutiko exekuzioa eragin. Ahultasun horretarako, CVE-2020-27654 identifikatzailea esleitu da.

Gainerako ahultasunetarako, honako identifikatzaileak esleitu dira: CVE-2019-11823, CVE-2020-27649, CVE-2020-27651, CVE-2020-27653, CVE-2020-27654, CVE-2020-27655, CVE-2020-27657 eta CVE-2020-27658.

Etiketak: Eguneratzea, Komunikazioak, Ahultasuna.

Segurtasun eguneratzea 5.5.2 WordPress-erako

Argitalpen data: 2020/10/30

Garrantzia: Altua

Kaltetutako baliabideak:

WordPress, 5.5.1 bertsioa eta aurrekoak.

Azalpena:

WordPress-en azken bertsioa argitaratu da, eta 10 segurtasun arazo konpondu dira horren bidez.

Konponbidea:

5.5.2 bertsiora eguneratzea.

Xehetasunak:

Segurtasun-zuzenketek konpontzen dituzten ahultasunen ondorioz, erasotzaileak honako aukerak izan litzake:

- Spam sartzea,
- XSS egitea (Cross-Site Scripting),
- XML-RPC bidez pribilegioetan gora egitea,
- RCE exekuzioa (Remote Command Execution),
- Artxiboak modu arbitrarioan ezabatzea,
- CSRF (Cross-Site Request Forgery) egitea.

Etiketak: Eguneratzea, CMS, Ahultasuna

Bufferrak gainezka egitea Windowsen kernel eremuan

Argitalpen data: 2020/11/03

Garrantzia: Kritikoa

Kaltetutako baliabideak:

Windowsen bertsio guztiak, Windows 7tik aurrera, Windows 10 bertsio berrienera arte.

Azalpena:

Mateusz Jurczyk eta Sergei Glazunovlek, Google Project Zero taldekoak, 0-day ahultasun bat antzeman dute Windows sistema eragilean. Une honetan, baliteke baten bat ahultasun hori erabiltzen aritzea, pribilegioetan gora egiteko.

Konponbidea:

- Windowsen 0-day ahultasun hori zuzentzeko eguneratzea azaroaren 10ean argitaratuko da.
- Google Chromeren ahultasuna bertsio honetan partxeatu zen: 86.0.4240.111.

Xehetasunak:

Windowsen kernel kriptografiaren kontrolagailuak, Windows Kernel Cryptography Driver (cng.sys) programetarako DeviceCNG gailu bat jarri du erakusgai erabiltzaile moduan dauden programetarako, eta IOCTL barietatea onartzen du, sarrera egitura ez tribialekin. Horren ondorioz, tokiko erasotzaile batek pribilegioetan gora egin lezake eta sandbox-etik irten. Ahultasun horretarako, CVE-2020-17087 identifikatzailea esleitu da.

Ahultasun hori baliatzeko, erasotzaileak Google Chromeko 0-day ahultasuna baliatzen ari dira aurretik. Horren identifikatzailea CVE-2020-15999 da, eta horrek Chromeren barruan kode maltzurra exekutatzeko aukera ematen die.

Etiketak: 0day, Ahultasuna, Windows.