Kalteberatasunak Cisco IOS-XRn

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EDUKI-TAULA

Erantzukizunetik salbuesteko klausula

Dokumentu hau Zibersegurtasunaren Euskal Agentziak erakundeen eta herritar interesatuen segurtasunaren alde beharrezkotzat jotzen dituen alertak gizarteratzeko helburuz sortu da. Zibersegurtasunaren Euskal Agentzia ezin da jo, inola ere, Zibersegurtasunerako Euskal Agentziaren webgunean emandako informazioaren edo erreferentzia egiten zaien teknologien erabilerak eragin ditzaketen kalteen erantzuletzat, ezta kanpoko web-orrialdeetarako esteka bidez sartutako bestelako informazioaren, software produktuen edo Zibersegurtasunaren Euskal Agentziaren webgunean edo alertan ager daitezkeen beste edozein informazioaren erantzuletzat ere. Edonola ere, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak iritzi eta gomendioak dira, hemen bildutako terminoekin bat etorrita, eta emandako informazioaren ondorioz ezingo da eragin juridiko loteslerik sortu.

Salmenta debekatzeko klausula

1. Laburpen exekutiboa

Ciscok segurtasun-abisuak argitaratu ditu **3 kalteberatasun** jorratzeko. **Cisco IOS-XR** produktuari eragiten diote kalteberatasun horiek, hau da, fabrikatzailearen datuen zentroko sistema eragileari. Honako identifikatzaileak dituzte: CVE-2024-20318, CVE-2024-20320 eta CVE-2024-20327. Kalteberatasun horiek larritasun handiko mehatxuak dira eta kaltetutako sistemen konfidentzialtasunari, eskuragarritasunari eta osotasunari eragin diezaiokete.

Bestalde, Ciscoren Produktuen Segurtasun Gorabeherei Erantzunetarako Taldeak (PSIRT) ez du inolako deskribatutako kalteberatasunaren erabilera gaiztoaren edo hedapenaren berririk.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneratzeak eta arintze-neurriak, eta, horrela, akats nabarmenak zuzendu ditu. Beraz, kalteberatasun horiek eta beste batzuk prebenitzeko, sistema eta aplikazioak eskuragarri dagoen azken bertsioaren arabera eguneratuta izatea gomendatzen da, dagozkien adabakiak argitaratu bezain laster.

2. Kaltetutako baliabideak

Argitaratutako lehen kalteberatasunaren identifikatzailea CVE-2024-20318 da eta Cisco produktu hauei eragiten die:

- Lightspeed edo Lightspeed-Plusen oinarritutako lineako txartela instalatuta duten ASR 9000 serieko routerrak (gehitzeko zerbitzuen routerrak).
- ASR9902 serieko errendimendu handiko router konpaktuak.
- ASR9903 serieko errendimendu handiko router konpaktuak.
- IOS XRd vRouters.
- IOS XRv 9000 Routers.

Argitaratutako bigarren kalteberatasunaren identifikatzaileaCVE-2024-20320 da eta honako produktu hauei eragiten die, baldin eta Cisco IOS-OS softwarearen bertsio kalteberaren bat exekutatzen ari badira:

- 8000 serieko routerrak.
- IOS XRd Control Plane.
- IOS XRd vRouter.
- NCS540L irudiak exekutatzen ari diren NCS 540 serieko routerrak.
- NCS 5700 serieko routerrak (NCS-57B1-5DSE-SYS, NCS-57B1-6D24-SYS y NCS-57C1-48Q6-SYS).

Argitaratutako hirugarren kalteberatasunaren identifikatzailea CVE-2024-20327 da eta Cisco IOS XR softwarearen bertsio kaltebera bat exekutatzen ari diren eta ezaugarri hauek dituzten Ciscoren ASR 9000 Serieko Zerbitzuak Gehitzeko Routerrei eragiten die:

- Instalatutako Lightspeed edo Lightspeed-Plusen oinarritutako lineako txartela.
- BNG gaitutako PPPoErekin.
- Kaltetutako lineako txartelean gaitutako PPPoE duen interfaze edo azpi-interfaze bat gutxienez.
- Kaltetutako lineako txartelean gaitutako PPPoE ez duen interfaze edo azpi-interfaze bat gutxienez.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

CVE-2024-20320: Cisco IOS XR-ren SSH bezeroaren kalteberatasuna. Cisco 8000 serieko routerrei eta Cisco Network Convergence System (NCS) 540 eta 5700 serieko routerrei eragiten die. Kalteberatasun hori arrakastaz ustiatuz gero, egiaztatutako tokiko erasotzaile batek pribilegioak igo ditzake kaltetutako gailu batera. Kalteberatasun horren jatorrian dago SSH bezeroaren CLI komandoarekin gehitutako argudioen baliozkotze desegokia. Kaltetutako gailu batera lehentasun gutxiko erasotzaile bat sartuz gero, kalteberatasun hori aprobetxa dezake eta SSH bezeroaren komando manipulatua igorri komandoen lineako interfazearen bitartez (CLI).

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-266: Incorrect Privilege Assignment

Oinarrizko CVSSa: **7.8**

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- **Eraso-bektorea:** Bertakoa
- **Erasoaren konplexutasuna**: **Baxua**
- **Beharrezko pribilegioak: Baxuak**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: Aldaketarik gabe
- **Konfidentzialtasuna Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2024-20318: kalteberatasuna Cisco IOS XR-ren 2. geruzako Ethernet zerbitzuetan. Kalteberatasun hori ustiatuz gero, egiaztatu gabeko erasotzaile batek eragin dezake lineako txartelaren sareko prozesadore bat berrabiaraztea. Hori eginez gero, zerbitzua ukatuko litzateke (DoS).

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-20: Improper Input Validation

Oinarrizko CVSSa: **7.4**

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Eraso-bektorea:** Ondokoa
- **Erasoaren konplexutasuna**: **Baxua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: **Aldaketekin**

- **Konfidentzialtasuna** Bat ere ez
- **Integritatea:** Bat ere ez
- **Eskuragarritasuna: Altua**

CVE-2024-20327**:** Kalteberatasuna Cisco IOS XRko Etherneten (PPPoE) gaineko PPPren amaieraren funtzioan. ASR 9000 serieko gehitzeko zerbitzuko routerrei eragiten die. Kalteberatasun horren jatorria da Lightspeed edo Lightspeed-Plusen oinarritutako lineako txartelean PPPoE amaiera duen banda zabaleko sare baterako (BNG) sarbidearen funtzionalitatea exekutatzen ari den router batean jasotako eta gaizki eratutako PPPoE paketeak modu desegokian erabiltzea.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-266: Improper Input Validation

Oinarrizko CVSSa: **7.4**

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Eraso-bektorea:** Ondokoa
- **Erasoaren konplexutasuna**: **Baxua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: **Aldaketekin**
- **Konfidentzialtasuna** Bat ere ez
- **Integritatea:** Bat ere ez
- **Eskuragarritasuna: Altua**

4. Arintzea / Konponbidea

Ciscok doako software-eguneratzeak argitaratu ditu, abisu honetan deskribatutako kalteberatasunei aurre egiteko. Zerbitzu-kontratuak dituzten eta, hortaz, softwarearen eguneratze erregularrak jasotzen dituzten bezeroek ohiko eguneratze-kanalen bidez eskuratu behar dituzte segurtasun-zuzenketak.

5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2024-20318.
- CVE-2024-20320.
- CVE-2024-20327.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY