Kalteberatasunak Cisco NX-OSen

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EDUKI-TAULA

Erantzukizunetik salbuesteko klausula

Salmenta debekatzeko klausula

1. Laburpen exekutiboa

Ciscok segurtasun-abisuak argitaratu ditu **larritasun handiko 2 kalteberatasunekin** lotuta. **Cisco NX-OS** produktuari eragiten diote kalteberatasun horiek, hau da, fabrikatzailearen datuen zentroko sistema eragileari. Honako identifikatzaileak dituzte: CVE-2024-20321 eta CVE-2024-20267. Kalteberatasun horiek larritasun handiko mehatxuak dira Ciscoren produktuentzat, eta kaltetutako sistemen eskuragarritasunari 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 lehenengo kalteberatasunak, CVE-2024-20321 identifikatzailea duenak, Nexus 3600 serieko switchei eta Nexus 9500 R serieko lineako txartelei eragiten die, honako adierazleak dituztenei:

- N3K-C36180YC-R
- N3K-C3636C-R
- N9K-X9624D-R2
- N9K-X9636C-R
- N9K-X9636C-RX
- N9K-X9636Q-R
- N9K-X96136YC-R

Argitaratutako bigarren kalteberatasunak, CVE-2024-20267 identifikatzaileak duenak, honako produktu hauei eragiten die, baldin eta Cisco NX-OS softwarearen bertsio kalteberaren bat exekutatzen ari badira eta MPLS konfiguratuta badute:

- Nexus 3000 serieko switchak.
- Nexus 5500 plataformako switchak.
- Nexus 5600 plataformako switchak.
- Nexus 6000 serieko switchak.
- Nexus 7000 serieko switchak.
- Nexus 9000 serieko switchak, NX-OS “standalone” moduan dutenak.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

CVE-2024-20321: zerbitzua ukatzen duen kalteberatasuna. eBGP protokoloaren (External Border Gateway Protocol) ezarpenari eragiten dio Cisco NX-OSen. Partekatutako hardware bateko abiadura mugatzeko ilara bati esleitutako eBGP trafikoa kudeatzeko moduan du jatorria kalteberatasun honen arrazoiak. Kaltetutako gailu baten bidez ezaugarri jakin batzuk dituen sareko trafiko handia bidalita ustiatu dezake erasotzaileak kalteberatasun hau. Hala, sarean DoS zerbitzua ukatzea eragingo luke.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-400: Uncontrolled Resource Consumption

Oinarrizko CVSSa: **8.6**

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

- **Eraso-bektorea: Sarea**
- **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-2024-20267: zerbitzua ukatzen duen kalteberatasuna. Trafikoaren kudeaketari eragiten dio Cisco NX-OSn. Sartzen diren MPSL markoak prozesatzean gertatzen diren akatsak ez egiaztatzean du jatorria. Urruneko erasotzaile batek kalteberatasun hau ustiatu lezake MPLSrentzat gaitutako interfaze batera (helburuko gailukoa) MPLS marko baten barruan kapsulatutako Ipv6 pakete manipulatu bat bidalita. Ustiaketa arrakastatsua balitz, DoS zerbitzua ukatuko litzateke.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-120: Buffer Copy without Checking Size of Input

Oinarrizko CVSSa: **8.6**

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

- **Eraso-bektorea: Sarea**
- **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-2024-20321.
- CVE-2024-20267.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY