cyber zaintza
BASQUE CYBERSECURITY AGENCY

Kalteberatasunak Cisco Secure Clienten

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

EDUKI-TAULA

Erantzukizunetik salbuesteko klausula

Salmenta debekatzeko klausula

1. Laburpen exekutiboa

Ciscok segurtasun-abisuak argitaratu ditu **Cisco Secure Clienten larritasun handiko 2 kalteberatasun** tratatzeko**.** Honako hauek dira kalteberatasunen identifikatzaileak: CVE-2024-20338, CVE-2024-20337. Kalteberatasun horien ustiapena hori mehatxu oso larria da kaltetuak izan daitezkeen sistemen konfidentzialtasunari dagokionez.

Ciscoren Produktuen Segurtasun Jazoerei Erantzuteko Taldeak (PSIRT) ez du deskribatutako kalteberatasunen erabilera gaiztoaren edo hedapenaren gaineko inolako berririk.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneratzeak eta arintze-neurriak, eta, horrela, akats nabarmenak zuzendu ditu. Beraz, kalteberatasun hori eta beste batzuk prebenitzeko, gomendagarria da sistemak eta aplikazioak beti eskuragarri dagoen azken bertsioarekin gaurkotuta izatea.

2. Kaltetutako baliabideak

CVE-2024-20338 kalteberatasunaren kasuan:

- Linuxerako Cisco Secure Clienten bertsio kaltebera bat exekutatzen duten eta ISE Posture moduloa instalatuta duten Cisco gailuak.

CVE-2024-20337 kalteberatasunaren kasuan:

- Linuxerako Cisco Secure Client.
- MacOS-erako Cisco Secure Client.
- Windowserako Cisco Secure Client.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

CVE-2024-20337: Cisco Secure Clienteko SAML kautotze-prozesuari eragiten dion kalteberatasuna. Kautotu gabeko urruneko erasotzaile batek orga-itzulera eta lerro-jauzia komandoen injekzio-eraso bat (CRLF) egin dezake erabiltzaile baten aurka. Erabiltzaileak emandako sarreraren baliozkotze eskasa dago kalteberatasun honen oinarrian. Hala, erasotzaile batek kalteberatasun hau aprobetxa lezake, eta erabiltzaile bat esteka manipulatu batean klik egiteko konbentzitu, VPN saio bat ezartzen duen bitartean. Ustiapena arrakastatsua izanez gero, erasotzaileak script kode arbitrario bat exekuta lezake nabigatzailean, edo nabigatzailean oinarritutako informazio garrantzitsua eskura lezake; esaterako, baliozko SAML token bat. Gero erasotzaileak token hori erabili lezake urruneko sarbiderako VPN saio bat ezartzeko, kaltetutako erabiltzailearen pribilegioekin.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE 93: Improper Neutralization of CRLF Sequences

Oinarrizko CVSSa: **8.2**

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

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

CVE-2024-20338: Linuxerako Cisco Secure Clienteko ISE Posture moduluari eragiten dion kalteberatasuna. Bilaketa-ibilbideko kontrolatu gabeko elementu bat erabiltzean du jatorria kalteberatasun honek. Erasotzaile batek kalteberatasun hori aprobetxa lezake liburutegiko fitxategi gaizto bat fitxategien sistemako direktorio zehatz batean kopiatzeko eta administratzailea prozesu jakin bat berrabiarazi dezan konbentzitzeko. Arrakastaz ustiatuz gero, erasotzaileak kode arbitrario bat exekuta lezake kaltetutako gailu batean, root pribilegioekin.

Kalteberatasunen azterketaren neurketak honako hauek ditu:

CWE 427: Uncontrolled Search Path Element

Oinarrizko CVSSa: **7.3**

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

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

4. Arintzea / Konponbidea

Ohikoa den bezala, kalteberatasun horiek eta beste batzuk prebenitzeko, sistemak eta aplikazioak beti eskuragarri dagoen azken bertsiora eguneratuta izatea gomendatzen da, dagozkien eguneratzeak argitaratu bezain laster.

Honako bertsio hauetara eguneratzea gomendatzen da:

- Cisco Secure Client 4.10.04065 eta hurrengoak: eguneratu 4.10.08025 bertsiora.
- Cisco Secure Client 5.1: eguneratu 5.1.2.42 bertsiora.
- Linuxerako Cisco Secure Client, 5.1.2.42 baino lehenagoko bertsioak: eguneratu 5.1.2.42 bertsiora.

5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2024-20337
- CVE-2024-20338.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY