ClamAVren OLE2 artxiboko kalteberatasuna, Cisco produktuetan eragina duena.

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

EDUKI-TAULA

Erantzukizunetik salbuesteko klausula

Salmenta debekatzeko klausula

1. Laburpen exekutiboa

Ciscok segurtasun-abisu bat argitaratu du **larritasun handiko** kalteberatasun bat tratatzeko **ClamAV**ren **OLE2** fitxategi-formatuaren analizatzailean. Akats horren bidez, autentifikatu gabeko urrutiko erasotzaile batek zerbitzu-ukapeneko egoera bat sortzea ahalbidetu lezake. Identifikatzaile hau du: CVE-2024-20290. Akatsa larritasun handiko mehatxu izan daiteke Ciscoren produktutarako eta kaltetutako sistemen konfidentzialtasunean, osotasunean eta eskuragarritasunean eragina izan dezake.

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

Fabrikatzaileak argitaratu ditu jada eguneratzeak eta dagozkion arintze-neurriak, eta hala, zuzendu du nabarmendutako akatsa. Beraz, kalteberatasun hori eta beste batzuk prebenitzeko, gomendagarria da sistemak eta aplikazioak beti eskuragarri dagoen azken bertsioarekin gaurkotuta izatea.

2. Kaltetutako baliabideak

- Secure Endpoint Connector for Windows, bertsio honen aurrekoak: 7.5.17 (Feb 2024) 8.2.3.30119.
- Secure Endpoint Private Cloud, 3.8.0 bertsioaren aurrekoak.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunaren xehetasunak hauek dira:

CVE-2024-20290Kalteberatasun horren bidez, erasotzaile batek eragin dezake Windowserako Cisco Secure Endpoint Connector, Cisco Secure Endpoint Private Cloud sistematik banatzen dena, begizta batean sartzea eta erantzuteari uztea, eta hala, DoS egoera bat sortuz. Kalteberatasun hori analisian kate-amaierako balioak oker egiaztatzearen ondorio da, eta horrek heap bufferraren gainirakurketa eragin dezake. Erasotzaile batek kalteberatasun hori baliatu lezake kaltetutako gailu batean ClamaV bidez eskaneatzeko OLE2 edukia duen artxibo manipulatu bat bidalita. Exploit arrakastatsu baten bidez, erasotzaileak ClamAVren eskaneatze prozesua amaitu lezake, eta hala, kaltetutako softwarean DoS egoera bat sortuz eta sistemaren baliabide erabilgarriak kontsumituz.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-126: Buffer Over-read

Oinarrizko CVSSa: **7.5**

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

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

4. Arintzea / Konponbidea

Ohikoa den bezala, kalteberatasun hau eta beste batzuk prebenitzeko, gomendagarria da sistemak eta aplikazioak beti eskuragarri dagoen azken bertsioarekin eguneratuta izatea.

Kalteberatasun horiek konpontzeko, Ciscok software bertsio egoki batera eguneratzeko gomendatu die bere bezeroei:

- Secure Endpoint Connector for Windowserako, bertsio honetara eguneratzea: 7.5.17 (Feb 2024) 8.2.3.30119.
- Secure Endpoint Private Cloud sistemarako, 3.8.0 bertsiora eguneratzea, konektore eguneratuekin.

5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2024-20290.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY