Kalteberatasun kritikoak FortiOS eta FortiClientEMS sistemetan

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EDUKI-TAULA

1. Resumen ejecutivo 3
2. Recursos afectados 4
3. Análisis técnico 5
4. Mitigación / Solución 7
5. Referencias Adicionales 8

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

Fortinetek hainbat segurtasun-abisu argitaratu ditu **larritasun kritikoko 2 kalteberatasun** tratatzeko. Horien identifikatzaileak CVE-2024-23113 eta CVE-2024-21762 dira, eta **FortiOS produktuari** eragiten diote. Horrez gain, **larritasun handiko kalteberatasun bat** ere argitaratu du, CVE-2023-45581 identifikatzailea duena, eta **FortiClientEMS** produktuari eragiten diona. Kalteberatasun hori mehatxu oso larria da kaltetuak izan daitezkeen sistemen konfidentzialtasunari, osotasunari eta eskuragarritasunari dagokionez.

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

- FortiOS 6.0 bertsio guztiak.
- FortiOS 6.2, 6.2.0 bertsiotik 6.2.15 bertsiora.
- FortiOS 6.4, 6.4.0 bertsiotik 6.4.14 bertsiora.
- FortiOS 7.0, 7.0.0 bertsiotik 7.0.13 bertsiora.
- FortiOS 7.2, 7.2.0 bertsiotik 7.2.6 bertsiora.
- FortiOS 7.4, 7.4.0 bertsiotik 7.4.2 bertsiora.
- FortiClientEMS 6.2 bertsio guztiak.
- FortiClientEMS 6.4 bertsio guztiak.
- FortiClientEMS 7.0, 7.0.0 bertsiotik 7.0.4 bertsiora.
- FortiClientEMS 7.0, 7.0.6 bertsiotik 7.0.10 bertsiora.
- FortiClientEMS 7.2, 7.2.0 bertsiotik 7.2.2 bertsiora.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

CVE-2024-23113: kanpotik kontrolatutako formatu katearen kalteberatasuna FortiOSen fgfmd deamon-en. Horren bidez, baimenik gabeko urrutiko erasotzaile batek kodea edo komando arbitrarioak exekutatu litzake, bereziki diseinatutako eskaeren bidez.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE 134: Use of Externally-Controlled Format String

Oinarrizko CVSSa: **9.8**

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**

CVE-2024-21762: Mugetatik kanpoko idazketaren kalteberatasuna FortiOS-en. Horren bidez, baimenik gabeko urrutiko erasotzaile batek kodea edo komando arbitrarioak exekutatu ditzake, bereziki diseinatutako HTTP eskaeren bidez.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE 787: Out-of-bounds Write

Oinarrizko CVSSa: **9.6**

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**

CVE-2023-45581: pribilegioen kudeaketa desegokiaren kalteberatasuna FortiClientEMSen interfaze administratibo grafikoan. Horren bidez, Super Administratzaile pribilegioak dituen webgunearen administratzaile batek beste

gune batzuei eragiten dieten eragiketa administratibo globalak egin litzake, manipulatutako HTTP edo HTTPS eskaeren bidez.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE 269: Improper Privilege Management

Oinarrizko CVSSa: **7.9**

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

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

4. Murriztea / Konponbidea

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

CVE-2024-23113 ahultasuna zuzentzeko, Fortinetek hau gomendatzen du:

- FortiOS 7.0 eguneratzea 7.0.14 bertsiora edo ondorengo batera.
- FortiOS 7.2 eguneratzea 7.2.7 bertsiora edo ondorengo batera.
- FortiOS 7.4 eguneratzea 7.4.3 bertsiora edo ondorengo batera.

CVE-2024-21762 ahultasuna zuzentzeko, Fortinetek hau gomendatzen du:

- Migratu FortiOS 6.0 bertsio zuzendu batera.
- FortiOS 6.2 eguneratzea 6.2.16 bertsiora edo ondorengo batera
- FortiOS 6.4 eguneratzea 6.4.15 bertsiora edo ondorengo batera.
- FortiOS 7.0 eguneratzea 7.0.14 bertsiora edo ondorengo batera.
- FortiOS 7.2 eguneratzea 7.2.7 bertsiora edo ondorengo batera.
- FortiOS 7.4 eguneratzea 7.4.3 bertsiora edo ondorengo batera.

CVE-2023-45581 ahultasuna zuzentzeko, Fortinetek hau gomendatzen du:

- FortiClientEMS 6.2 eta FortiClientEMS 6.4 migratzea bertsio zuzendu batera.
- FortiClientEMS 7.0 eguneratzea 7.0.11 bertsiora edo ondorengo batera.
- FortiClientEMS 7.2 eguneratzea 7.2.3 bertsiora edo ondorengo batera.

5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2024-21762
- CVE-2024-23113
- CVE-2023-45581


cyber
zaintza
BASQUE CYBERSECURITY AGENCY