Kalteberatasun kritikoak FortiOS eta FortiClientEMS sistemetan

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

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

Fortinetek hainbat segurtasun-abisu argitaratu ditu **larritasun kritikoa duten 3 kalteberatasun** jorratzeko, eta hauek dira identifikatzaileak: CVE-2023-42789, CVE-2023-42790 eta CVE-2023-48788. Kalteberatasun horiek **FortiOS produktuari** eragiten diote. **Larritasun handiko beste 3 kalteberatasun** ere argitaratu ditu, CVE-2023-47534, CVE-2024-23112 eta CVE-2023-36554, eta horiek **FortiClientEMS** produktuari eragiten diote.

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

- FortiClientEMS 7.2 7.2.0 bertsiotik 7.2.2 bertsiora.
- FortiClientEMS 7.0 7.0.0 bertsiotik 7.0.10 bertsiora.
- FortiClientEMS 6.4 bertsio guztiak.
- FortiClientEMS 6.2 bertsio guztiak.
- FortiClientEMS 6.0 bertsio guztiak.
- FortiOS 7.4.0 bertsiotik 7.4.1 bertsiora.
- FortiOS 7.2.0 bertsiotik 7.2.5 bertsiora.
- FortiOS 7.0.0 bertsiotik 7.0.12 bertsiora.
- FortiOS 6.4.0 bertsiotik 6.4.14 bertsiora.
- FortiOS 6.2.0 bertsiotik 6.2.15 bertsiora.
- FortiProxy 7.4.0 bertsioa
- FortiProxy 7.2.0 bertsiotik 7.2.6 bertsiora.
- FortiProxy 7.0.0 bertsiotik 7.0.12 bertsiora.
- FortiProxy 2.0.0 bertsiotik 2.0.13 bertsiora.
- FortiOS 7.2 7.2.0 bertsiotik 7.2.6 bertsiora.
- FortiOS 7.0 7.0.1 bertsiotik 7.0.13 bertsiora.
- FortiOS 6.4, 6.4.7 bertsiotik 6.4.14 bertsiora.
- FortiProxy 7.4, 7.4.0 bertsiotik 7.4.2 bertsiora.
- FortiProxy 7.2, 7.2.0 bertsiotik 7.2.8 bertsiora.
- FortiProxy 7.0, 7.0.0 bertsiotik 7.0.14 bertsiora.
- FortiManager 7.4.0 bertsioa
- FortiManager 7.2.0 bertsiotik 7.2.3 bertsiora.
- FortiManager 7.0.0 bertsiotik 7.0.10 bertsiora.
- FortiManager 6.4.0 bertsiotik 6.4.13 bertsiora.
- FortiManager 6.2 bertsio guztiak.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

CVE-2023-42789: **Fortinet FortiOS** eta **Fortinet FortyProxyren** bertsio hauei eragiten dien mugez kanpo idazteko kalteberatasuna:

- FortiOS 7.4.0 bertsiotik 7.4.1 bertsiora.
- FortiOS 7.2.0 bertsiotik 7.2.5 bertsiora.
- FortiOS 7.0.0 bertsiotik 7.0.12 bertsiora.
- FortiOS 6.4.0 bertsiotik 6.4.14 bertsiora.
- FortiOS 6.2.0 bertsiotik 6.2.15 bertsiora.
- FortiProxy 7.4.0
- FortiProxy 7.2.0 bertsiotik 7.2.6 bertsiora.
- FortiProxy 7.0.0 bertsiotik 7.0.12 bertsiora.
- FortiProxy 2.0.0 bertsiotik 2.0.13 bertsiora.

Kalteberatasun hori ustiatuz gero, erasotzaile batek baimenik gabeko kodeak edo komandoak exekutatu ditzake berariaz diseinatutako HTTP eskarien bidez.

Kalteberatasunen azterketaren neurketak honako hauek ditu:

CWE-787: Out-of-bounds Write

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-2023-42790: **FortiOS** eta **FortiProxyren** atari gatibuko pilan oinarritutako buferrak gainezka egitea eragiten duen kalteberatasuna. Barneko erasotzailea atari horretara sar daiteke eta kode edo komando arbitrarioak exekuta ditzake bereziki diseinatutako HTTP eskarien bidez.

Hauek dira **FortiOS** eta **FortiProxyren** kaltetutako bertsioak:

- FortiOS 7.4.0 bertsiotik 7.4.1 bertsiora.
- FortiOS 7.2.0 bertsiotik 7.2.5 bertsiora.
- FortiOS 7.0.0 bertsiotik 7.0.12 bertsiora.
- FortiOS 6.4.0 bertsiotik 6.4.14 bertsiora.
- FortiOS 6.2.0 bertsiotik 6.2.15 bertsiora.

- FortiProxy 7.4.0
- FortiProxy 7.2.0 bertsiotik 7.2.6 bertsiora.
- FortiProxy 7.0.0 bertsiotik 7.0.12 bertsiora.
- FortiProxy 2.0.0 bertsiotik 2.0.13 bertsiora.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-121: Stack-based Buffer Overflow

Oinarrizko CVSSa: **8.1**

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-2023-48788: FortiClientEMSko SQL komando batean (SQL Injection) erabilitako elementu bereziak modu okerrean neutralizatzen dituen kalteberatasuna da eta baimenik gabeko erasotzaile batek baimenik gabeko kodea edo komandoak exekutatu ditzake espezifikoki egindako eskarien bidez.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

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-2023-47534: Fortinet FortiClientEMSko CSV artxibo batean formula-elementuak modu desegokian neutralizatzeagatik eragindako kalteberatasuna. Kalteberatasun hori ustiatuz gero, erasotzaile batek baimenik gabeko kodeak edo komandoak exekutatu ditzake berariaz diseinatutako paketeen bidez.

Hauek dira FortiClientEMSren kaltetutako bertsioak:

- FortiClientEMS 7.2.0 bertsiotik 7.2.2 bertsiora.
- FortiClientEMS 7.0.0 bertsiotik 7.0.10 bertsiora.
- FortiClientEMS 6.4.0 bertsiotik 6.4.9 bertsiora.
- FortiClientEMS 6.2.0 bertsiotik 6.2.9 bertsiora.
- FortiClientEMS 6.0.0 bertsiotik 6.0.8 bertsiora.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-1236: Improper Neutralization of Formula Elements in a CSV File

Oinarrizko CVSSa: **9.6**

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

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

CVE-2024-23112: Erabiltzaileak FortiOS eta FortiProxy SSLVPNn kontrolatutako gakoaren bidez baimena omititzeagatik eragindako kalteberatasuna da eta egiaztatutako erasotzaile batek beste erabiltzaile baten markagailurako sarbidea lor dezake URL bat manipulatuz.

Hauek dira FortiOS eta FortiProxyren kaltetutako bertsioak:

- FortiOS 7.4.0 bertsiotik 7.4.1 bertsiora.
- FortiOS 7.2.0 bertsiotik 7.2.6 bertsiora.
- FortiOS 7.0.1 bertsiotik 7.0.13 bertsiora.
- FortiOS 6.4.7 bertsiotik 6.4.14 bertsiora.
- FortiProxy 7.4.0 bertsiotik 7.4.2 bertsiora.
- FortiProxy 7.2.0 bertsiotik 7.2.8 bertsiora.
- FortiProxy 7.0.0 bertsiotik 7.0.14 bertsiora.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-639: Authorization Bypass Through User-Controlled Key

Oinarrizko CVSSa: **8.0**

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

- **Eraso-bektorea:** Ondokoa
- **Erasoaren konplexutasuna:** Altua

- **Beharrezko pribilegioak: Baxua**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena: Aldaketekin**
- **Konfidentzialtasuna Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2023-36554: FortiManagerrerako FortiWLM MEAn sarbide-kontrol okerreko kalteberatasuna da eta egiaztatu gabeko urruneko erasotzaile batek kode edo komando arbitrarioak exekutatu ditzake berariaz diseinatutako eskaeren bidez.

Hauek dira FortiManagerren kaltetutako bertsioak:

- FortiManager 7.4.0 bertsioa
- FortiManager 7.2.0 bertsiotik 7.2.3 bertsiora.
- FortiManager 7.0.0 bertsiotik 7.0.10 bertsiora.
- FortiManager 6.4.0 bertsiotik 6.4.13 bertsiora.
- FortiManager 6.2 bertsio guztiak.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-284: Improper Access Control

Oinarrizko CVSSa: **8.1**

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna:** Altua
- **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 horiek eta beste batzuk prebenitzeko, sistemak eta aplikazioak beti eskuragarri dagoen azken bertsiora eguneratuta izatea gomendatzen da, dagozkien eguneratzeak argitaratu bezain laster.

CVE-2023-42789 eta CVE-2023-42790 kalteberatasunak zuzentzeko, honakoa gomendatzen du Fortinetek:

- FortiOS 7.4.0 bertsiora edo ondorengo batera eguneratzea
- FortiOS 7.4.2 bertsiora edo ondorengo batera eguneratzea
- FortiOS 7.2.6 bertsiora edo ondorengo batera eguneratzea
- FortiOS 7.0.13 bertsiora edo ondorengo batera eguneratzea
- FortiOS 6.4.15 bertsiora edo ondorengo batera eguneratzea
- FortiOS 6.2.16 bertsiora edo ondorengo batera eguneratzea
- FortiProxy 7.4.1 bertsiora edo ondorengo batera eguneratzea
- FortiProxy 7.2.7 bertsiora edo ondorengo batera eguneratzea
- FortiProxy 7.0.13 bertsiora edo ondorengo batera eguneratzea
- FortiProxy 2.0.14 bertsiora edo ondorengo batera eguneratzea

CVE-2023-48788 kalteberatasuna zuzentzeko, Fortinetek hau gomendatzen du:

- FortiClientEMS 7.2.3 bertsiora edo altuagora eguneratzea
- FortiClientEMS 7.0.11 bertsiora edo altuagora eguneratzea

CVE-2023-47534 kalteberatasuna zuzentzeko, Fortinetek hau gomendatzen du:

- FortiClientEMS 7.2 bertsiotik 7.2.3 bertsiora edo ondorengo batera eguneratzea
- FortiClientEMS 7.0 bertsiotik 7.0.11 bertsiora edo ondorengo batera eguneratzea
- FortiOS 6.4 bertsio zuzendu batera migratzea
- FortiOS 6.2 bertsio zuzendu batera migratzea
- FortiOS 6.0 bertsio zuzendu batera migratzea

CVE-2024-23112 kalteberatasuna zuzentzeko, Fortinetek hau gomendatzen du:

- FortiOS 7.4 bertsiotik 7.4.2 bertsiora edo ondorengo batera eguneratzea
- FortiOS 7.2 bertsiotik 7.2.7 bertsiora edo ondorengo batera eguneratzea
- FortiOS 7.0 bertsiotik 7.0.14 bertsiora edo ondorengo batera eguneratzea
- FortiOS 6.4 bertsiotik 6.4.15 bertsiora edo ondorengo batera eguneratzea
- FortiProxy 7.4 bertsiotik 7.4.3 bertsiora edo ondorengo batera eguneratzea
- FortiProxy 7.2 bertsiotik 7.2.9 bertsiora edo ondorengo batera eguneratzea
- FortiProxy 7.0 bertsiotik 7.0.15 bertsiora edo ondorengo batera eguneratzea

CVE-2023-36554 kalteberatasuna zuzentzeko, Fortinetek hau gomendatzen du:

- FortiManager 7.4.1 bertsiora edo ondorengo batera eguneratzea
- FortiManager 7.2.4 bertsiora edo ondorengo batera eguneratzea
- FortiManager 7.0.11 bertsiora edo ondorengo batera eguneratzea
- FortiManager 6.4.14 bertsiora edo ondorengo batera eguneratzea

5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2023-42789.
- CVE-2023-42790.
- CVE-2023-48788.
- CVE-2023-47534.
- CVE-2024-23112.
- CVE-2023-36554.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY