# Larritasun handiko kalteberatasunak Ivantiren produktuetan

CYBERZAINTZA-ABISUAK

**TLP: CLEAR**

www.zibersegurtasun.eus

## 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

**Ivantik** segurtasun-abisu bat argitaratu du **larritasun handiko bi kalteberatasun** tratatzeko: CVE-2024-21888, pribilegioetan eskalatzekoa, eta CVE-2024-21893, Server-Side Request Forgery (SSRF). Akats horiek **Ivanti Policy Secure Gateways**, **Ivanti Connect Secure** eta **Ivanti Neurons for ZTA** produktuei eragiten diete, eta, ustiatuz gero, larritasun kritikoko mehatxua izan litezke Ivantiren hainbat produkturentzat, eta eragina izan dezake kaltetutako sistemen konfidentzialtasunean.

Oraingoz, publiko egin dira fabrikatzailearen murrizketa- edo konponbide-neurriak, kalteberatasunak konponduko dituzten segurtasun-eguneratzeak iritsi bitartean.

## 2. Kaltetutako baliabideak

- Ivanti Connect Secure 9.x, 22.x.
- Ivanti Connect Secure 9.x, 22.x.
- Ivanti Neurons for ZTA.

## 3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

CVE-2024-21888: pribilegioetan gora egiteko kalteberatasuna Ivanti Connect Secure (9.x, 22.x) eta Ivanti Policy Secure (9.x, 22.x) gailuen web osagaian; horri esker, erabiltzaile batek pribilegioak administrari pribilegioetara igo ditzake.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **8.8**

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

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

CVE-2024-21893: Server-Side Request Forgery (SSRF) motako kalteberatasuna (zerbitzariaren aldeko eskaerak faltsutzea), Ivanti Connect Secure (9.x, 22.x) eta Ivanti Policy Secure (9.x, 22.x) eta Ivanti Neurons for ZTA-ren SAML osagaian. Horren bidez, erasotzaile bat baliabide mugatu batzuetara sar daiteke, baimenik gabe.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE 918: Server-Side Request Forgery (SSRF)

Oinarrizko CVSSa: **8.2**

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

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

## 4. Murriztea / Konponbidea

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

Ivantik jakinarazi du partxeak deskargatzeko eskuragarri daudela deskarga estandarreko atariaren bidez Ivanti Connect Secure-rako (9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2 eta 22.5R1.1 bertsioak) eta ZTA 22.6R1.3. bertsiorako.

Bestalde, fabrikatzaileak nabarmendu du funtsezkoa dela bezeroek neurriak berehala hartzea erabat babestuta daudela ziurtatzeko. Horretarako, bezeroek KB Article dokumentua kontsulta dezakete konponbide-neurriak nola aplikatu jakiteko.

## 5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2024-21888.
- CVE-2024-21893.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY