cyber zaintza
BASQUE CYBERSECURITY AGENCY

Kalteberatasun kritikoak Ivantiren produktuetan

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

Ivantik segurtasun-abisuak argitaratu ditu **larritasun kritikoko 2 kalteberatasun** jorratzeko: CVE-2023-46808 **egiaztatutako artxiboen urruneko idazketa** eragiten duena eta CVE-2023-41724 **kodea urrunetik exekutatzen duena**. Kalteberatasun horiek ITSM **Ivanti Neurons** produktuei eta **Ivanti Standalone Sentry**ri eragiten diote, hurrenez hurren. Akatsa larritasun kritikoko mehatxu izan daiteke eta kaltetutako sistemen konfidentzialtasunean, osotasunean eta eskuragarritasunean eragina izan dezake.

Bestalde, Ivantik jakinarazi du ez dagoela ebidentziarik adierazteko kalteberatasun horiek aktiboki ustiatu direnik.

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

- Ivanti Neurons ITSM 2023.1, 2023.2, 2023.3rako
- Ivanti Standalone Sentry 9.17.0, 9.18.0 eta 9.19.0 (aurreko bertsioak ere arriskuan daude).

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunaren xehetasunak hauek dira:

CVE-2023-46808: asmo txarreko eragileek aukera izan dezakete direktorio sentiberetan artxiboak idazteko, eta, ondorioz, webguneko aplikazioko erabiltzailearen testuinguruan komandoak exekuta ditzakete. Ekintza hori egiteko, asmo txarreko norbanakoa aldez aurretik egiaztatu behar du sistemak.

Kalteberatasun horrek Ivanti Neuronsekin bateragarriak diren ITSMrako bertsio guztiei eragiten die (2023.3, 2023.2 eta 2023.1).

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **9.9**

CVSS:3.0/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-2023-41724: Kodea urrunetik exekutatzeko kalteberatasuna da eta sare fisiko edo logiko berean dagoen asmo txarreko eragile bati aukera ematen dio gailuaren sistema operatiboan komandoak arbitrarioki ustiatzeko.

Kalteberatasunak **Ivanti Standalone Sentryrekin** (9.17.0, 9.18.0 eta 9.19.0) bateragarriak diren bertsio guztiei eta bertsio zahar eta ez bateragarriei eragiten die (9.17.0 bertsioaren aurrekoak).

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **9.6**

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

- **Eraso-bektorea:** Ondokoa
- **Erasoaren konplexutasuna**: **Baxua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: **Aldaketekin**
- **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.

Ivantik jakinarazi du CVE-2023-46808 kalteberatasunaren kasuan adabaki bat dagoela ITSMrako Ivanti Neuronsekin bateragarriak diren bertsio guztientzat (2023.3, 2023.2 eta 2023.1).

CVE-2023-41724 kalteberatasunaren kasuan, Ivantik jakinarazi du Ivanti Standalone Sentry 9.17.0, 9.18.0 eta 9.19.0rekin bateragarriak diren bertsio guztientzako aplikagarria den adabaki bat dagoela eskuragarri.

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-2023-46808.
- CVE-2023-41724.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY